МЕЖДУНАРОДНЫЙ СТАНДАРТ

ИСО/МЭК 27001

Первое издание
2005-10-15

Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования

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

Номер для ссылки
ISO/IEC 27001:2005(E)

Содержание

таблицы

Предисловие

ИСО (Международная организация по стандартизации) и МЭК (Международная электротехническая комиссия) образуют специализированную систему всемирной стандартизации. Государственные органы, являющиеся членами ИСО или МЭК, участвуют в разработке международных стандартов посредством технических комитетов, учрежденных соответствующей организацией для того, чтобы обсуждать определенные области технической деятельности. Технические комитеты ИСО и МЭК сотрудничают в областях взаимного интереса. Другие международные организации, правительственные и неправительственные, контактирующие с ИСО и МЭК, также принимают участие в работе. В области информационных технологий, ИСО и МЭК учредили Совместный технический комитет, ISO/IEC JTC 1.

Проекты международных стандартов составляются в соответствии с правилами, определенными директивами ИСО/МЭК, часть 2.

В области информационных технологий ИСО и МЭК учредили Совместный технический комитет (JTC), ISO/IEC JTC 1. Проекты международных стандартов, принятые объединенным техническим комитетом, рассылаются государственным органам на голосование. Для опубликования документа в качестве международного стандарта необходимо как минимум 75% голосов членов-организаций, принимающих участие в голосовании.

Обращаем внимание на то, что некоторые элементы этого документа могут быть предметом патентных прав. ИСО и МЭК не несут ответственность за установление какого-либо или всех таких патентных прав.

ISO/IEC 27001 был подготовлен Совместным техническим комитетом ISO/IEC JTC 1, *Информационные технологии*, Подкомитет SC 27, *Методики защиты ИТ*.

Данное первое издание ISO/IEC 90003 отменяет и заменяет ISO 9000-3:1997, которое было усовершенствовано с целью соответствия ISO 9001:2000. ISO 9000-3:1997 находилось в зоне ответственности Технического комитета (ТК) ISO/TC 176/SC 2.

Введение

0.1 Общие положения

Этот международный стандарт был подготовлен для того, чтобы предоставить модель для создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшения Системы Менеджмента Защиты Информации (СМЗИ). Рекомендуется, чтобы принятие СМЗИ было стратегическим решением для организации. На проектирование и реализацию СМЗИ организации влияют ее потребности и цели, требования защиты, применяемые процессы, а также размер и структура организации. Ожидается, что все эти элементы, а также их вспомогательные системы будут со временем меняться. Ожидается, что реализация СМЗИ будет масштабироваться в соответствии с потребностями организации, например, простая ситуация требует простого решения СМЗИ.

Этот международный стандарт можно использовать для оценки соответствия заинтересованными внутренними и внешними сторонами.

0.2 Процессный подход

Этот международный стандарт принимает процессный подход для создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшения СМЗИ организации.

Организации нужно идентифицировать много видов деятельности и управлять ими для того, чтобы функционировать результативно. Любой вид деятельности, использующий ресурсы и управляемый для того, чтобы дать возможность преобразования входов в выходы, можно считать процессом. Часто выход одного процесса непосредственно образует вход следующего процесса.

Применение системы процессов в рамках организации, вместе с идентификацией и взаимодействием этих процессов, а также их управлением, может называться «процессный подход».

Процессный подход к менеджменту защиты информации, представленный в данном международном стандарте, помогает пользователям подчеркнуть важность следующего:

a) понимание требований защиты информации и потребности установить политику и цели для защиты информации организации;

b) средства реализации и управления для менеджмента рисками организации, связанными с защитой информации, в контексте общих деловых рисков организации;

c) постоянный контроль и анализ качества исполнения и результативности СМЗИ; и

d) непрерывное улучшение, основанное на объективном измерении.

Этот международный стандарт принимает модель «Plan-Do-Check-Act» (PDCA[1]), которая применяется для структуризации всех процессов СМЗИ. На рисунке 1 показано, как СМЗИ берет в качестве входных данных требования защиты информации и ожидания заинтересованных сторон и посредством необходимых действий и процессов выдает результаты по защите информации, которые удовлетворяют этим требованиям и ожиданиям. На рисунке 1 также показаны связи и процессы, представленные в Разделах 4, 5, 6, 7 и 8.

Принятие модели PDCA также будет отражать принципы, установленные в Руководящих указаниях OECD (2002)[2], управляющих защитой информационных систем и сетей. Этот международный стандарт обеспечивает прочную модель для реализации принципов, приведенных в тех руководящих указаниях, управляющих оценкой риска, проектированием и реализацией защиты, менеджментом и переоценкой защиты.

ПРИМЕР 1

Требование может быть таковым, что нарушения защиты информации не приведут к серьезному финансовому ущербу для организации и/или вызовут затруднения у организации.

ПРИМЕР 2

Ожидание может быть таковым, что если происходит серьезный инцидент – возможно, взлом Web-сайта электронного бизнеса организации, – то должны быть люди, обладающие достаточной подготовкой по соответствующим процедурам для минимизации негативного влияния.

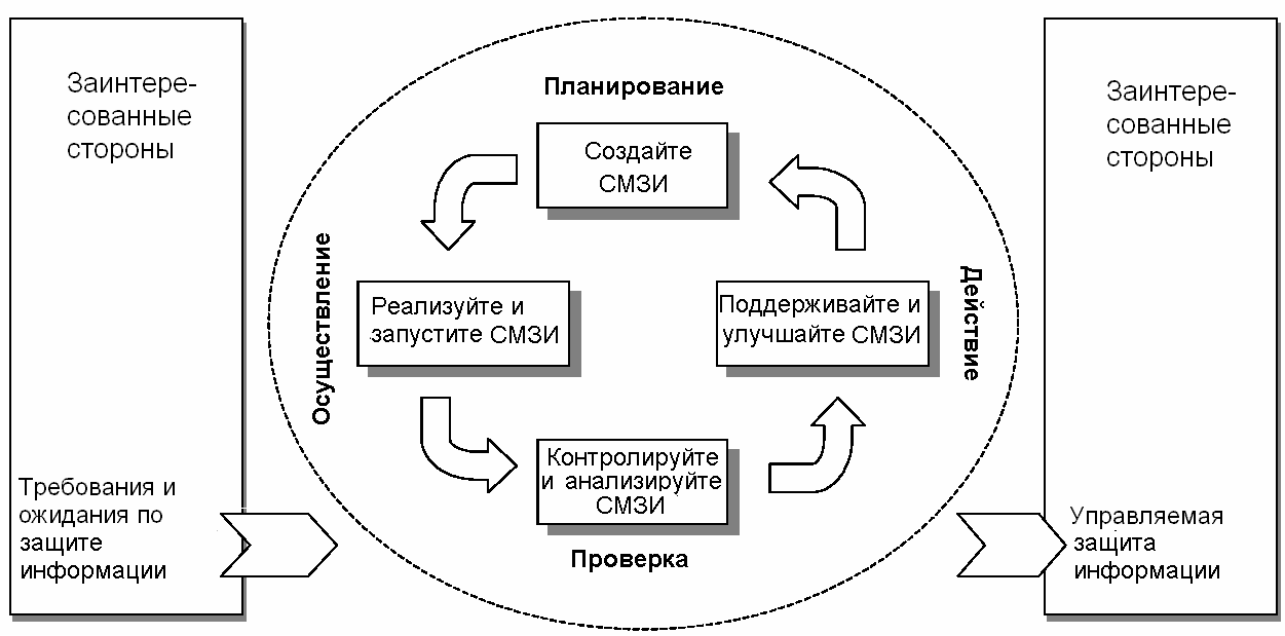

Рисунок 1 — Модель PDCA, примененная к процессам СМЗИ

[1] цикл Шухарта-Деминга (планирование – осуществление – проверка – действие) (*Прим. переводчика*)

[2] OECD *Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security*. Paris: OECD, July 2002. www.oecd.org

Планирование (создайте СМЗИ)	Установите политику, цели, процессы и процедуры, относящиеся к менеджменту рисков и улучшению защиты информации для выдачи результатов в соответствии с общей политикой и целями организации.
Осуществление (внедрите и эксплуатируйте СМЗИ)	Реализуйте и эксплуатируйте политику, средства управления, процессы и процедуры в области СМЗИ;
Действие (постоянно контролируйте и анализируйте СМЗИ):	Оценивайте и, где применимо, измеряйте показатели процессов по отношению к политике, целям и практическому опыту в области СМЗИ, доложите результаты руководству для анализа.
Проверка (поддерживайте в рабочем состоянии и улучшайте СМЗИ)	Осуществляйте корректирующие и предупреждающие действия, основанные на результатах внутреннего аудита СМЗИ и анализа со стороны руководства, или на другой значимой информации для того, чтобы достичь постоянного улучшения СМЗИ.

0.3 Совместимость с другими системами менеджмента

Этот международный стандарт совмещен с ISO 9001:2000 и ISO 14001:2004 для того, чтобы поддерживать согласованную и комплексную реализацию и работу со связанными стандартами менеджмента. Одна должным образом разработанная система менеджмента может, таким образом, удовлетворить требованиям всех этих стандартов. В таблице C.1 показана взаимосвязь между разделами данного международного стандарта, ISO 9001:2000 и ISO 14001:2004.

Этот международный стандарт предназначен для того, чтобы способствовать организации совместить или интегрировать ее СМЗИ с имеющими к ней отношение требованиями системы менеджмента качества.

Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования

ВАЖНО — Эта публикация не имеет целью включить в себя все необходимые положения договора. Пользователи являются ответственными за его правильное применение. Соответствие международному стандарту само по себе не дает иммунитета от правовых обязательств.

1 Область приложения

1.1 Общие положения

Этот международный стандарт охватывает все типы организаций (например, коммерческие предприятия, государственные органы, некоммерческие организации). Этот международный стандарт определяет требования для создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшения документированной СМЗИ в контексте общих деловых рисков организации. Он определяет требования для реализации средств управления защитой, приспособленных к потребностям отдельных организаций или их подразделений.

СМЗИ разрабатывается для того, чтобы обеспечить выбор адекватных и пропорциональных средств управления защитой, которые защищают информационные активы и придают уверенность заинтересованным сторонам.

ПРИМЕЧАНИЕ 1: Ссылки на «бизнес», «дело» [business] в этом международном стандарте следует интерпретировать, в общих чертах, как означающие те виды деятельности, которые являются основными для существования организации.

ПРИМЕЧАНИЕ 2: В ISO/IEC 17799 даны руководящие указания по реализации, которое могут быть использованы при проектировании средств управления.

1.2 Применение

Требования, установленные в этом международном стандарте, носят общий характер и предназначены для применения ко всем организациям, независимо от типа, размера и характера. Исключение какого-либо из требований, определенных в Разделах 4, 5, 6, 7, и 8, не приемлемо, если организация заявляет о соответствии этому международному стандарту.

Любое исключение из средств управления, которое, как выясняется, необходимо для удовлетворения критерию приемлемости риска, необходимо обосновать, и необходимо предоставить подтверждение того, что связанные с этим риски были

приняты подотчетными лицами. Если исключаются какие-либо средства управления, то заявления о соответствии этому международному стандарту неприемлемы, за исключением тех случаев, когда такие исключения не влияют на способность и/или ответственность организации обеспечить защиту информации, которая удовлетворяет требованиям защиты, определяемым оценкой риска и применимыми законодательными или нормативными требованиями.

ПРИМЕЧАНИЕ: Если организация уже имеет действующую систему менеджмента деловых процессов (например, по отношению к ISO 9001 или ISO 14001), то в большинстве случаев предпочтительно выполнять требования этого международного стандарта в рамках этой существующей системы менеджмента.

2 Нормативные ссылки

Перечисленные ниже документы необходимы для применения этого документа. Для датированных ссылок, подходит только указанное издание. Для недатированных ссылок, подходит самое последнее издание упомянутого документа (включая любые изменения).

ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

3 Термины и определения

Для целей этого документа, применяются следующие термины и определения.

3.1
актив [asset]
что-либо, что имеет ценность для организации

[ISO/IEC 13335-1:2004]

3.2
доступность [availability]
свойство быть доступным и годным к употреблению по требованию уполномоченного лица

[ISO/IEC 13335-1:2004]

3.3
конфиденциальность [confidentiality]
свойство, что информация не сделана доступной или не разглашена неуполномоченным лицам, организациям или процессам

[ISO/IEC 13335-1:2004]

3.4
защита информации [information security]
сохранение конфиденциальности, целостности и доступности информации; кроме того, также могут быть включены другие свойства, такие как аутентичность, подотчетность, неотрекаемость и надежность

[ISO /IEC 17799:2005]

3.5
событие в системе защиты информации [information security event]
выявленный случай системы, услуги или состояния сети, указывающий на возможное нарушение политики защиты информации или нарушения в работе средств защиты, или прежде неизвестная ситуация, которая может иметь значение для защиты

[ISO /IEC TR 18044:2004]

3.6
инцидент в системе защиты информации [information security incident]
одно или серия нежелательных или неожиданных событий в системе защиты информации, которые имеют большой шанс скомпрометировать деловые операции и поставить под угрозу защиту информации

[ISO/IEC TR 18044:2004]

3.7
система менеджмента защиты информации
СМЗИ
[information security management system]
[ISMS]
часть общей системы менеджмента, основанной на подходе деловых рисков, с целью создать, внедрить, эксплуатировать, постоянно контролировать, анализировать, поддерживать в рабочем состоянии и улучшать защиту информации,

ПРИМЕЧАНИЕ: Система менеджмента включает организационную структуру, политику, деятельность по планированию, ответственность, практики, процедуры, процессы и ресурсы.

3.8
целостность [integrity]
свойство оберегания точности и полноты активов

[ISO/IEC 13335-1:2004]

3.9
остаточный риск [residual risk]
риск, остающийся после обработки риска

[ISO/IEC Guide 73:2002]

3.10
принятие риска [risk acceptance]
решение взять на себя риск

[ISO/IEC Guide 73:2002]

3.11
анализ риска [risk analysis]
систематическое использование информации для выявления источников и для оценки степени риска

[ISO/IEC Guide 73:2002]

3.12
оценка риска [risk assessment]
целостный процесс анализа риска и оценки значительности риска

[ISO/IEC Guide 73:2002]

3.13
оценка значительности риска [risk evaluation]
процесс сравнения расчетного риска с заданными критериями риска, с целью определить значительность риска

[ISO/IEC Guide 73:2002]

3.14
менеджмент рисков [risk management]
согласованные виды деятельности по руководству и управлению организацией в отношении рисков

[ISO/IEC Guide 73:2002]

3.15
обработка риска [risk treatment]
процесс выбора и реализации мер по изменению риска

[ISO/IEC Guide 73:2002]

ПРИМЕЧАНИЕ: В этом международном стандарте термин «управление» [«control»] используется как синоним для термина «мера» [«measure»].

3.16
заявление о применимости [statement of applicability]
документированное заявление, описывающее цели и средства управления, которые имеют отношение и применимы к СМЗИ организации.

ПРИМЕЧАНИЕ: Цели управления и средства управления основываются на результатах и выводах оценки рисков и процесса обработки рисков, законодательных или нормативных требованиях, договорных обязательствах и деловых требованиях защиты информации организации.

4 Система менеджмента защиты информации

4.1 Общие требования

Организация должна создать, внедрить, эксплуатировать, постоянно контролировать, анализировать, поддерживать в рабочем состоянии и улучшать документированную СМЗИ в контексте целостной деловой деятельности организации и рисков, с которыми она сталкивается. Для целей этого международного стандарта, используемый процесс основан на модели PDCA, показанной на рисунке 1.

4.2 Создание и менеджмент СМЗИ

4.2.1 Создать СМЗИ

Организация должна сделать следующее.

a) Определить область приложения и границы СМЗИ в терминах характеристик бизнеса, организации, ее местоположения, активов и технологий, также включая подробности и обоснования любых исключений из области применения (см. п.1.2).

b) Определить политику в отношении СМЗИ в терминах характеристик бизнеса, организации, ее местоположения, активов и технологий, которая:

   1) включает в себя структуру для установки целей и устанавливает общий смысл руководства и принципов действия в отношении защиты информации;

   2) учитывает деловые и законодательные или нормативные требования, а также договорные обязательства по защите;

   3) равняется на контекст стратегического менеджмента рисков организации, в котором будет происходить создание СМИЗ и поддержание СМЗИ в рабочем состоянии;

   4) устанавливает критерии, по которым будет оцениваться значительность риска (см. п.4.2.1c)); и

   5) была утверждена руководством.

   ПРИМЕЧАНИЕ: Для целей этого международного стандарта, политика в отношении СМЗИ рассматривается как расширенная версия политики в области защиты информации. Обе эти политики можно описать в одном документе.

c) Определить подход к оценке риска в организации.

   1) Определить методологию оценки риска, которая подходит для СМЗИ, а также соответствует установленным деловым требованиям защиты информации, законодательным и нормативным требованиям.

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

Выбранная методология оценки риска должна гарантировать, что оценки риска дают сравнимые и воспроизводимые результаты.

ПРИМЕЧАНИЕ: Есть различные методологии оценки риска. Примеры методологий оценки риска обсуждаются в ISO/IEC TR 13335-3, I*nformation technology — Guidelines for the management of IT Security — Techniques for the management of IT Security*.

d) Выявить риски.

1) Выявить активы в рамках области приложения СМЗИ, а также владельцев[3] этих активов.

2) Выявить угрозы для этих активов.

3) Выявить уязвимые места, которые могут быть использованы угрозами.

4) Выявить негативные влияния, которые потери конфиденциальности, целостности и доступности могут оказать на активы.

e) Проанализировать риск и оценить значительность риска.

1) Оценить деловые негативные влияния на организацию, которые могут быть результатом сбоев в защите, принимая во внимание последствия потери конфиденциальности, целостности или доступности активов.

2) Оценить реалистичную вероятность случаев нарушения защиты, происходящих в свете преобладающих угроз и уязвимых мест, и негативные влияния, связанные с этими активами, а также реализуемые на текущий момент средства управления.

3) Оценить уровни риска.

4) Определить, являются ли риски приемлемыми или требуют обработки с использованием критериев принятия риска, установленных в п.4.2.1c)2).

f) Выявить и оценить возможности для обработки рисков.

Возможные действия включают следующее:

1) применение подходящих средств управления;

2) сознательное и объективное принятие рисков, при условии, что они четко соответствуют политике организации и удовлетворяют критериям для принятия рисков (см. п.4.2.1c)2));

3) избегание риска; и

4) передача связанных деловых рисков другим сторонам, например, страховщикам, поставщикам.

[3] Термин «владелец» означает личность или объект, которые утвердили ответственность руководства за управление производством, разработкой, поддержанием в рабочем состоянии, использованием и защитой активов. Термин «владелец» не означает, что человек действительно имеет какие-либо права собственности в отношении актива.

g) Выбрать цели управления и средства управления для обработки риска.

Цели управления и средства управления должны быть выбраны и реализованы, с целью удовлетворить требованиям, выявленным процессом оценки рисков и обработки рисков. Этот выбор должен учитывать критерии для принятия рисков (см. п.4.2.1c)2)), а также законодательные, нормативные и договорные требования.

Выбор целей управления и средств управления из Приложения А должен быть частью этого процесса; они должны выбираться как подходящие для того, чтобы охватить выявленные требования.

Списки целей управления и средств управления, приведенные в Приложении А, не являются исчерпывающими, также можно выбрать дополнительные цели управления и средства управления.

ПРИМЕЧАНИЕ: В Приложении А содержится всеобъемлющий список целей управления целей и средств управления, которые, как было обнаружено, обычно значимы в организациях. Пользователи этого международного стандарта направляются к Приложению А как к отправной точке для выбора управления, с целью гарантировать, что ни одна из важных возможностей управления не была упущена.

h) Получить утверждение руководства предлагаемого остаточного риска.

i) Получить разрешение руководства на реализацию и работу СМЗИ.

j) Подготовить Заявление о применимости.

Должно быть подготовлено заявление о применимости, которое включает в себя следующее:

1) цели управления и средства управления, выбранные в п.4.2.1g), а также причины их выбора;

2) цели управления и средства управления, реализуемые на данный момент (см. п.4.2.1e)2)); и

3) исключение любых целей управления и средств управления из Приложения А, а также обоснование для их исключения.

ПРИМЕЧАНИЕ: Заявление о применимости представляет собой свод решений, касающихся обработки рисков. Обоснование исключений обеспечивает перекрестный контроль того, что никакие средства управления не были неумышленно опущены.

4.2.2 Реализовать и эксплуатировать СМЗИ

Организация должна сделать следующее.

a) Сформулировать план обработки рисков, в котором были бы определены подходящие действия по менеджменту, ресурсы, ответственность и приоритеты для менеджмента рисками защиты безопасности (см. раздел 5).

b) Реализовать план обработки рисков для того, чтобы достичь определенных целей управления, что включает в себя учет финансирования и распределения ролей и ответственности.

c) Реализовать средства управления, выбранные в п.4.2.1g), с целью достичь целей управления.

d) Определить, как измерять результативность выбранных средств управления или группы средств управления, а также определить, как эти измерения предстоит использовать для оценки результативности управления так, чтобы выдать сравнимые и воспроизводимые результаты (см. п.4.2.3c)).

ПРИМЕЧАНИЕ: Измерение результативности средств управления позволяет менеджерам и персоналу определять, насколько хорошо средства управления достигают запланированных целей управления.

e) Осуществлять подготовку и программы повышения осведомленности (см. п.5.2.2).

f) Осуществлять менеджмент эксплуатации СМЗИ.

g) Управлять ресурсами для СМЗИ (см. п.5.2).

h) Внедрить процедуры и другие средства управления, способные дать возможность быстрого обнаружения события в системе защиты информации и реакции на инциденты в системе защиты информации (см. п.4.2.3a)).

4.2.3 Постоянно контролировать и анализировать СМЗИ

Организация должна сделать следующее.

a) Выполнять процедуры постоянного контроля и анализа, а также другие средства управления для того, чтобы:

   1) быстро обнаруживать ошибки в результатах обработки;

   2) быстро выявлять предпринимаемые и успешные нарушения защиты и инциденты;

   3) дать руководству возможность определять, осуществляются ли виды деятельности по защите, назначенные людям или осуществляемые информационной технологией, как ожидалось;

   4) помогать обнаруживать события в системе защиты информации и тем самым предотвращать инциденты в системе защиты информации путем использования индикаторов; и

   5) определять, были ли действия, предпринятые для улаживания проблемы с нарушением защиты, результативными.

b) Предпринимать регулярный анализ результативности СМЗИ (включая соответствие политике и целям СМЗИ, а также анализ средств управления защитой), принимая во внимание результаты аудитов защиты, инциденты, результаты измерений результативности, предложения и обратную реакцию всех заинтересованных сторон.

c) Измерять результативность средств управления для того, чтобы проверить, что требования защиты были удовлетворены.

d) Анализировать оценки риска через запланированные интервалы и анализировать остаточные риски и определенные приемлемые уровни риска, принимая во внимание изменения в следующем:

   1) организация;

   2) технология;

   3) деловые цели и процессы;

   4) выявленные угрозы;

   5) результативность реализованных средств управления; и

   6) внешние события, такие как изменения в законодательной или нормативно-правовой среде, измененные договорные обязательства, а также изменения в социальном климате.

e) Проводить внутренние аудиты СМЗИ через запланированные интервалы (см. раздел 6).

ПРИМЕЧАНИЕ: Внутренние аудиты, иногда называемые аудиты, проводимые первой стороной, проводятся организацией, или от ее имени, самой организацией для внутренних целей.

f) Регулярно осуществлять анализ СМЗИ со стороны руководства, с целью гарантировать, что область применения остается адекватной, и выявляются улучшения в процессе СМЗИ (см. п.7.1).

g) Обновлять планы защиты для того, чтобы учесть данные, полученные в ходе деятельности по постоянному контролю и анализу.

h) Записывать действия и события, которые могли оказать негативное влияние на результативность или качество работы СМЗИ (см. п.4.3.3).

4.2.4 Поддерживать в рабочем состоянии и улучшать СМЗИ

Организация должна регулярно делать следующее.

a) Внедрять выявленные улучшения в СМЗИ.

b) Осуществлять надлежащие корректирующие и предупреждающие действия в соответствии с п.8.2 и п.8.3. Применять уроки, полученные из опыта защиты других организаций, а также из опыта самой организации.

c) Сообщать обо всех действиях и улучшениях всем заинтересованным сторонам с уровнем детальности, соответствующим обстоятельствам и, по значимости, согласовывать дальнейшие действия.

d) Гарантировать, что улучшения достигают предполагаемых целей.

4.3 Требования к документации

4.3.1 Общие положения

Документация должна включать записи о решениях руководства, обеспечивать прослеживаемость действий до решений руководства и политики, а также обеспечивать воспроизводимость результатов.

Важно быть способными продемонстрировать взаимосвязь от выбранных средств управления обратно до результатов процесса оценки рисков и обработки рисков, а затем до политики и целей СМЗИ.

Документация СМЗИ должна включать следующее:

a) документированное заявление о политике (см. п.4.2.1b)) и целях СМЗИ;

b) область приложения СМЗИ (см. п.4.2.1a));

c) процедуры и средства управления в поддержку СМЗИ;

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

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

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

g) документированные процедуры, необходимые организации для того, чтобы гарантировать результативное планирование, работу и управление ее процессами защиты информации, а также для того, чтобы описать, как измерять результативность средств управления (см. п.4.2.3c));

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

i) Заявление о применимости.

ПРИМЕЧАНИЕ 1: Там, где в этом международном стандарте встречается термин «документированная процедура», он означает, что процедура создана, документально подтверждена, реализована и поддерживается в рабочем состоянии.

ПРИМЕЧАНИЕ 2: Объем документации по СМЗИ может различаться от организации к организации, по следующим причинам:

— размер организации и тип ее деятельности; и

— область приложения и сложность требований защиты и системы, менеджмент которой осуществляется.

ПРИМЕЧАНИЕ 3: Документы и записи могут быть в любой форме или на любом носителе информации.

4.3.2 Управление документами

Документы, требуемые СМЗИ, должны быть защищены и должны управляться. Документированная процедура должна быть создана для определения действий руководства, необходимых для следующего:

a) утверждать документы на адекватность перед выпуском;

b) анализировать и обновлять документы, по необходимости, а также повторно утверждать документы;

c) гарантировать, что указаны изменения и текущий статус редакции документов;

d) гарантировать, что имеющие отношение к делу версии применимых документов доступны в местах использования;

e) гарантировать, что документы остаются разборчивыми и легко идентифицируемыми;

f) гарантировать, что документы доступны тем, кому они нужны, и что они перемещаются, хранятся, и, в конце концов, ликвидируются в соответствии с процедурами, применимыми к их классификации;

g) гарантировать, что документы внешнего происхождения идентифицированы;

h) гарантировать, что распространение документов управляется;

i) предотвращать неумышленное использование устаревших документов; и

j) применять подходящую идентификацию к ним, если они сохраняются для какой-либо цели.

4.3.3 Управление записями

Записи должны создаваться и поддерживаться в рабочем состоянии для того, чтобы обеспечивать подтверждение соответствия требованиям и результативной работы СМЗИ. Они должны быть защищены и должны управляться. СМЗИ должна учитывать любые имеющие отношение к делу законодательные или нормативные требования, а также договорные обязательства. Записи должны оставаться разборчивыми, легко идентифицируемыми и извлекаемыми. Средства управления, необходимые для идентификации, хранения, защиты, поиска, а также сроки хранения и ликвидации записей должны быть документированы и реализованы.

В записях должны быть отражены показатели процесса, указанные в п.4.2, а также все эпизоды значительных инцидентов в системе безопасности, связанные со СМЗИ.

ПРИМЕР

Примерами записей являются книга посетителей, протокол аудита и заполненные формы разрешения доступа.

5 Ответственность руководства

5.1 Обязательства руководства

Руководство должно предоставлять подтверждение своих обязательств по созданию, внедрению, эксплуатации, постоянному контролю, анализу, поддержанию в рабочем состоянии и улучшению СМЗИ путем следующих действий:

a) создание политики СМЗИ;

b) обеспечение создания целей и планов СМЗИ;

c) определение ролей и ответственности в области защиты информации;

d) доведение до сведения организации важности выполнения целей защиты информации и соответствия политике защиты информации, ответственности организации в соответствии с законом и потребности организации в непрерывном улучшении;

e) обеспечение достаточного количества ресурсов для создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшения СМЗИ (см. п.5.2.1);

f) принятие решения о критериях принятия риска и приемлемых уровнях риска;

g) обеспечение проведения внутренних аудитов СМЗИ (см. раздел 6); и

h) проведение анализа со стороны руководства СМЗИ (см. раздел 7).

5.2 Менеджмент ресурсов

5.2.1 Обеспечение ресурсами

Организация должна определить и обеспечивать ресурсы, которые необходимы для следующего:

a) создать, внедрить, эксплуатировать, постоянно контролировать, анализировать, поддерживать в рабочем состоянии и улучшать СМЗИ;

b) гарантировать, что процедуры защиты информации поддерживают деловые требования;

c) выявить и рассматривать законодательные и нормативные требования, а также договорные обязательства по защите;

d) поддерживать в рабочем состоянии адекватную защиту путем правильного применения всех реализованных средств управления;

e) проводить анализ, когда это необходимо, и соответствующим образом реагировать на результаты этого анализа; и

f) где необходимо, улучшать результативность СМЗИ.

5.2.2 Подготовка, осведомленность и компетентность

Организация должна гарантировать, что весь персонал, которому назначена ответственность, определенная в СМЗИ, компетентен для выполнения требуемых задач, путем следующего:

a) определять необходимую компетентность для персонала, выполняющего работу, влияющую на СМЗИ;

b) обеспечивать подготовку или предпринимая другие действия (например, нанимая на работу компетентный персонал), с целью удовлетворить эти потребности;

c) оценивать результативность предпринятых действий; и

d) поддерживать в рабочем состоянии записи об образовании, подготовке, мастерстве, опыте и квалификации (см. п.4.3.3).

Организация должна также гарантировать, что весь имеющий отношение к делу персонал отдает себе отчет в значимости и важности их деятельности в области защиты информации и в том, какой вклад они вносят в достижение целей СМЗИ.

6 Внутренние аудиты СМЗИ

Организация должна проводить внутренние аудиты СМЗИ через запланированные интервалы, с целью определить следующее:

a) соответствуют ли требованиям этого международного стандарта и относящихся к ним законов или нормы;

b) соответствуют ли выявленным требованиям защиты информации;

c) эффективно ли реализуются и поддерживаются в рабочем состоянии; и

d) выполняются ли, как ожидается

цели управления, средства управления, процессы и процедуры СМЗИ организации.

Программа аудиты должна быть спланирована с учетом статуса и важности процессов и областей, которые нужно проверять, а также результатов предыдущих аудитов. Должны быть определены критерии, область приложения, частота и методы аудита. Выбор аудиторов и проведение аудитов должны гарантировать объективность и беспристрастность процесса аудита. Аудиторы не должны проверять свою собственную работу.

Ответственность за планирование и проведение аудитов и требования для планирования и проведения аудитов, а также для сообщения результатов и поддержания записей в рабочем состоянии (см. п.4.3.3), должны быть определены в документированной процедуре.

Руководство, ответственное за проверяемую область, должно гарантировать, что действия по устранению обнаруженных несоответствий и их причины предпринимаются без ненужной задержки. Последующая деятельность должна

включать в себя верификацию предпринятых действий и составление отчета по результатам верификации (см. раздел 8).

ПРИМЕЧАНИЕ: Документ ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*, может предоставить полезные руководящие указания по проведению внутренних аудитов СМЗИ.

7 Анализ СМЗИ со стороны руководства

7.1 Общие положения

Руководство должно анализировать СМЗИ организации через запланированные интервалы (по крайней мере, один раз в год), чтобы гарантировать ее постоянную пригодность, адекватность и результативность. Этот анализ должен включать в себя оценивание возможностей для улучшения и потребности в изменениях СМЗИ, включая политику защиты информации и цели защиты информации. Результаты анализа должны быть четко документированы, а записи должны поддерживаться в рабочем состоянии (см. п.4.3.3).

7.2 Входные данные для анализа

Входные данные для анализа со стороны руководства должны включать в себя следующее:

a) результаты аудитов и анализа СМЗИ;

b) обратная реакция заинтересованных сторон;

c) методики, продукты или процедуры, которые можно было бы использовать в организации для улучшения качества работы и результативности СМЗИ;

d) статус предупреждающих и корректирующих действий;

e) уязвимые места или угрозы, адекватно не рассмотренные в предыдущих оценках риска;

f) результаты измерений результативности;

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

h) любые изменения, которые могли повлиять на СМЗИ; и

i) рекомендации по улучшению.

7.3 Выходные данные анализа

Выходные данные анализа со стороны руководства должны включать в себя любые решения и действия, имеющие отношение к нижеследующему.

a) Улучшение результативности СМЗИ.

b) Обновление оценки риска и плана обработки риска.

c) Изменения процедур и средств управления, которые влияют на защиту информации, если это необходимо, для того чтобы среагировать на внутренние или внешние события, которые могли негативно повлиять на СМЗИ, включая изменения в следующем:

   1) деловые требования;

   2) требования защиты;

   3) деловые процессы, влияющие на существующие деловые требования;

   4) нормативные или законодательные требования;

   5) договорные обязательства; и

   6) уровни риска и/или критерии принятия риска.

d) Необходимые ресурсы.

e) Улучшение в том, как измеряется результативность средств управления.

8 Улучшение СМЗИ

8.1 Постоянное улучшение

Организация должна постоянно улучшать результативности СМЗИ посредством использования политики защиты информации, целей защиты информации, результатов аудита, анализа наблюдаемых событий, корректирующих и предупреждающих действий и анализа со стороны руководства (см. раздел 7).

8.2 Корректирующие действия

Организация должна предпринимать действия по устранению причины несоответствия требованиям СМЗИ для того, чтобы предотвращать повторение. Документированная процедура для корректирующего действия должна определять требования для следующего:

a) выявление несоответствий;

b) определение причин несоответствий;

c) оценивание потребности в действиях, чтобы гарантировать, что несоответствия не возникнут снова;

d) определение и реализация требующихся корректирующих действий;

e) записывание результатов предпринятых действий (см. п.4.3.3); и

f) анализ предпринятого корректирующего действия.

8.3 Предупреждающие действия

Организация должна определить действие для устранения причины возможного несоответствия требованиям СМЗИ для того, чтобы предотвратить его возникновение. Предпринятые предупреждающие действия должны соответствовать негативному влиянию возможных проблем. Документированная процедура для предупреждающего действия должна определять требования для следующего:

a) выявление возможных несоответствий и их причин;

b) оценивание потребности в действии, имеющем целью предотвратить случай несоответствия;

c) определение и реализация требуемого предупреждающего действия;

d) записывание результатов предпринятого действия (см. п.4.3.3); и

e) анализ предпринятого предупреждающего действия.

Организация должна выявить изменившиеся риски и определить требования к предупреждающим действиям, сосредоточив внимание на значительно изменившихся рисках.

Приоритет предупреждающих действий должен быть определен на основе результатов оценки риска.

ПРИМЕЧАНИЕ: Действие по предотвращению несоответствий часто является экономически более выгодным, чем корректирующее действие.

Приложение А
(обязательное)

Цели управления и средства управления

Цели управления и средства управления, перечисленные в таблице А.1, получены непосредственно из целей управления и средств управления, перечисленных в разделах 5—15 ISO/IEC 17799:2005, и равняются на них. Списки в таблице А.1 не являются исчерпывающими, и организация может счесть, что необходимы дополнительные цели управления и средства управления. Цели управления и средства управления из этих таблиц должны быть выбраны как часть процесса СМЗИ, определенного в 4.2.1.

В разделах 5—15 ISO/IEC 17799:2005 приведены советы и руководящие указания по лучшей практике поддержки средств управления, определенных в пп.А.5—А.15.

Таблица А.1 — Цели управления и средства управления

А.5	**Политика защиты**	
А.5.1	**Политика защиты информации**	
Цель:	Обеспечить направление и поддержку со стороны руководства для защиты информации в соответствии с деловыми требованиями, а также законами и нормами, имеющими отношение к делу.	
А.5.1.1	Документ политики в области защиты информации	*Управление* Документ политики в области защиты информации должен быть утвержден руководством, а также опубликован и доведен до сведения всех сотрудников и имеющих отношение к делу заинтересованных сторон
А.5.1.2	Анализ политики в области защиты информации	*Управление* Политика в области защиты информации должна анализироваться через запланированные интервалы или в случае возникновения значительных изменений, с целью гарантировать ее непрерывную пригодность, адекватность и результативность.

A.6 Организация защиты информации

A.6.1 Внутренняя организация

Цель: Осуществлять менеджмент защиты информации в рамках организации

A.6.1.1	Обязанности руководства по защите информации	*Управление* Руководство должно активно поддерживать защиту в пределах организации посредством четкого руководства, продемонстрированных обязательств, подробного распределения и признания ответственности за защиту информации.
A.6.1.2	Координация защиты информации	*Управление* Деятельность по защите информации должна быть скоординирована представителями различных частей организации с соответствующими ролями и рабочими функциями.
A.6.1.3	Распределение ответственности за защиту информации	*Управление* Вся ответственность за защиту информации должна быть четко определена.
A.6.1.4	Процесс получения разрешения для средств, обрабатывающих информацию	*Управление* Должен быть определен и реализован процесс менеджмента получений разрешения для новых средств, обрабатывающих информацию.
A.6.1.5	Соглашения конфиденциальности	*Управление* Требования к конфиденциальности или соглашения о неразглашении, отражающие потребности организации в защите информации, должны быть выявлены и должны регулярно анализироваться.
A.6.1.6	Контакты с властями	*Управление* Должны поддерживаться подходящие контакты с компетентными органами
A.6.1.7	Контакты со специальными группами	*Управление* Должны поддерживаться надлежащие контакты со специальными группами или другими форумами специалистов по защите, а также профессиональными ассоциациями.

A.6.1.8	Независимый анализ информационной безопасности	*Управление* Подход организации к менеджменту защиты информации и ее реализации (т.е. цели управления, средства управления, политика, процессы и процедуры для защиты информации) должны независимо анализироваться через запланированные интервалы, или когда происходят значительные изменения в реализации защиты.
A.6.2 Внешние стороны *Цель:* Поддерживать в рабочем состоянии защиту информации организации и средства, обрабатывающие информацию, которые доступны внешним сторонам, обрабатываются внешними сторонами, сообщены внешним сторонам или управляются внешними сторонами.		
A.6.2.1	Выявление рисков, связанных с внешними сторонами	*Управление* Должны быть выявлены риски для информации организации и средств, обрабатывающих информацию, проистекающие из деловых процессов, вовлекающих внешние стороны, а перед предоставлением доступа должны быть реализованы надлежащие средства управления.
A.6.2.2	Решение вопросов безопасности при работе с клиентами	*Управление* Все выявленные требования защиты должны быть рассмотрены до того, как клиентам будет предоставлен доступ к информации или активам организации.
A.6.2.3	Решение вопросов безопасности в соглашениях с третьими сторонами	*Управление* Соглашения с третьими сторонами, включающие доступ, обработку, сообщение или менеджмент информации организации или средств, обрабатывающих информацию, или добавление продуктов или услуг к средствам, обрабатывающим информацию, должны включать в себя все значимые требования защиты.

A.7 Менеджмент активов

A.7.1 Ответственность за активы

Цель: Достичь и поддерживать в рабочем состоянии подходящую защиту организационных активов.

A.7.1.1	Реестр активов	*Управление* Все активы должны быть четко определены, и должен быть составлен и должен поддерживаться в рабочем состоянии реестр всех важных активов.
A.7.1.2	Владение активами	*Управление* Вся информация и активы, связанные со средствами, обрабатывающими информацию, должны «находиться во владении»[4] назначенной части организации.
A.7.1.3	Приемлемое использование активов	*Управление* Должны быть определены, документированы и внедрены правила для приемлемого использования информации и активов, связанных со средствами, обрабатывающими информацию.

A.7.2 Классификация информации

Цель: Гарантировать, что информация получает подходящий уровень защиты.

A.7.2.1	Руководящие указания по классификации	*Управление* Информация должна быть классифицирована с точки зрения ее значения, законодательных требований, уязвимости и критичности для организации.
A.7.2.2	Маркировка и обработка информации	*Управление* В соответствии со схемой классификации, принятой организацией, должен быть разработан и реализован подходящий набор процедур маркировки и обработки информации.

[4] Пояснение: термин «владелец» означает личность или объект, которые утвердили ответственность руководства за управление производством, разработкой, поддержанием в рабочем состоянии, использованием и защитой активов. Термин «владелец» не означает, что человек действительно имеет какие-либо права собственности в отношении актива.

A.8 Защита человеческих ресурсов

A.8.1 Перед наймом на работу[5]

Цель: Гарантировать, что служащие, подрядчики и пользователи третьей стороны понимают свою ответственность и подходят для должностей, на которые они рассматриваются, а также снизить риск кражи, мошенничества или неправильного использования средств.

A.8.1.1	Роли и ответственность	*Управление* Роли и ответственность служащих, подрядчиков и пользователей третьей стороны в отношении защиты должны быть определены и задокументированы в соответствии с политикой защиты информации организации.
A.8.1.2	Экранирование	*Управление* Проверки верификации в фоновом режиме по всем кандидатам в служащие, в подрядчики и в пользователи третьей стороны должны проводиться в соответствии с имеющими отношение к делу законами, нормами и этикой, и должны быть пропорциональны деловым требованиям, классификации информации, которая будет доступной, и предполагаемым рискам.
A.8.1.3	Сроки и условия занятости	*Управление* Как часть договорного обязательства, служащие, подрядчики и пользователи третьей стороны должны согласиться и подписать сроки и условия договора личного найма, в котором должны быть указаны их ответственность за защиту информации и ответственность организации за защиту информации.

[5] Пояснение: Словосочетание «прием на работу» предназначено здесь для обозначения всех нижеследующих различных ситуаций: прием на работу людей (временно или долгосрочно), назначение должностей [job roles], изменение должностей, переуступка контрактов, а также прекращение любого из этих мероприятий.

A.8.2 Во время работы *Цель:* Гарантировать, что все служащие, подрядчики и пользователи третьей стороны осознают угрозы защите информации и хлопоты по защите информации, свою ответственность и свои обязательства, и оснащены для того, чтобы поддерживать организационную политику защиты во время своей обычной работы, а также для того, чтобы снизить риск человеческой ошибки.		
A.8.2.1	Ответственность руководства	*Управление* Руководство должно требовать от служащих, подрядчиков и пользователей третьей стороны применять защиту в соответствии с установленной политикой и процедурами организации.
A.8.2.2	Осведомленность, образование и подготовка в области защиты информации	*Управление* Все служащие организации и, если это имеет отношение к делу, подрядчики и пользователи третьей стороны, должны получить подходящую подготовку по повышению осведомленности и регулярные обновления организационной политики и процедур, насколько это имеет отношение к их рабочим функциям.
A.8.2.3	Дисциплинарный процесс	*Управление* Должен иметься дисциплинарный процесс для служащих, которые произвели нарушение защиты.
A.8.3 Окончание или изменение работы по найму *Цель:* Гарантировать, что служащие, подрядчики и пользователи третьей стороны уходят из организации или меняют службу упорядоченно.		
A.8.3.1	Ответственность за окончание работы по найму	*Управление* Должна быть четко определена и назначена ответственность за осуществление окончания или изменения работы по найму.
A.8.3.2	Возврат активов	*Управление* Все служащие, подрядчики и пользователи третьей стороны должны вернуть все активы организации, находящиеся в их владении, по окончании их работы по найму, договора или соглашения.

A.8.3.3	Удаление прав доступа	*Управление* Права доступа всех служащих, подрядчиков и пользователей третьей стороны к информации и средствам, обрабатывающим информацию, должны быть удалены по окончании срока их работы по найму, договора или соглашения, или же скорректированы при изменении.
A.9	**Физическая защита и защита от окружающей среды**	
A.9.1	**Зоны безопасности** *Цель:* Предотвратить неразрешенный физический доступ, ущерб и вмешательства в недвижимость и информацию организации.	
A.9.1.1	Физический периметр безопасности	*Управление* Для защиты зон, в которых находятся информация и средства, обрабатывающие информацию, должны использоваться периметры безопасности (барьеры, такие как стены, управляемый картами турникет на входе или контролируемая человеком вахта)
A.9.1.2	Средства управления физическим доступом	*Управление* Зоны безопасности должны быть защищены подходящими средствами управления входом, с целью гарантировать, что только персоналу, имеющему разрешение, позволен доступ.
A.9.1.3	Организация защиты офисов, комнат и оборудования	*Управление* Должна быть разработана и применена физическая защита офисов, комнат и оборудования.
A.9.1.4	Защита против внешних и экологических угроз	*Управление* Должна быть разработана и применена физическая защита против ущерба от огня, наводнения, землетрясения, взрыва, общественных беспорядков и других форм естественного или искусственного бедствия.
A.9.1.5	Работа в зонах безопасности	*Управление* Должна быть разработана и применена физическая защита и руководящие принципы для работы в зонах безопасности.

A.9.1.6	Зоны общего доступа, поставки и загрузки	*Управление* Места доступа, такие как зоны поставки и загрузки, а также другие места, где не имеющие разрешения лица могут войти в помещения, должны управляться и, если возможно, должны быть изолированы от средств, обрабатывающих информацию, с целью избежать неразрешенного доступа.
A.9.2 Защита оборудования *Цель:* Предотвратить гибель, ущерб, кражу или компрометацию активов и заминку в работе организации		
A.9.2.1	Размещение и защита оборудования	*Управление* Оборудование должно быть размещено или защищено так, чтобы снизить риски от угроз и опасностей окружающей среды, а также количество возможностей неразрешенного доступа.
A.9.2.2	Вспомогательное оборудование	*Управление* Оборудование должно быть защищено от нарушений энергоснабжения и других нарушений, вызванных сбоями во вспомогательном оборудовании.
A.9.2.3	Защита кабельной системы	*Управление* Источник энергии и кабели связи, по которым передаются данные или вспомогательные информационные услуги, должны быть защищены от перехвата или повреждения.
A.9.2.4	Техническое обслуживание оборудования	*Управление* Оборудование должно обслуживаться правильно, чтобы гарантировать постоянную доступность и целостность.
A.9.2.5	Защита оборудования вне помещений	*Управление* Защита должна быть применена к оборудованию вне помещений, с учетом различных рисков работы за пределами помещений организации.

A.9.2.6	Безопасная ликвидация или повторное использование оборудования	*Управление* Все единицы оборудования, содержащие носители информации, должны быть проверены, чтобы гарантировать, что любые уязвимые данные и лицензированное программное обеспечение было удалено или надежно перезаписано перед ликвидацией.
A.9.2.7	Перемещение собственности	*Управление* Оборудование, информация или программное обеспечение не должны выноситься [за пределы зоны безопасности] без предварительного разрешения.
A.10 Менеджмент средств связи и эксплуатации		
A.10.1 Процедуры эксплуатации и ответственность *Цель:* Гарантировать правильную и безопасную работу средств, обрабатывающих информацию.		
A.10.1.1	Документированные процедуры эксплуатации	*Управление* Процедуры эксплуатации должны быть документированы, поддерживаться в рабочем состоянии, и сделаны доступными для всех пользователей, которым они нужны.
A.10.1.2	Менеджмент изменений	*Управление* Изменения в средствах и системах, обрабатывающих информацию, должны управляться.
A.10.1.3	Разделение обязанностей	*Управление* Обязанности и области ответственности должны быть разделены, с целью снизить количество возможностей неразрешенного или непреднамеренного изменения или неправильного использования активов организации.
A.10.1.4	Разделение средств разработки, испытания и эксплуатации	*Управление* Средства разработки, испытания и эксплуатации должны быть разделены, с целью снизить риски неразрешенного доступа или изменений в системе эксплуатации.

A.10.2 Менеджмент предоставления услуг третьей стороны		
Цель: Реализовать и поддерживать подходящий уровень защиты информации и предоставления услуг в соответствии с соглашениями о предоставлении услуг третьей стороны.		
A.10.2.1	Предоставление услуг	*Управление* Должно быть гарантировано, что средства управления защитой, описания услуг и уровни предоставления, включенные в соглашение о предоставлении услуг третьей стороны, реализуются, эксплуатируются и поддерживаются третьей стороной.
A.10.2.2	Постоянный контроль и анализ услуг третьей стороны	*Управление* Услуги, отчеты и записи, предоставляемые третьей стороной, должны постоянно контролироваться и анализироваться; регулярно должны проводиться аудиты.
A.10.2.3	Менеджмент изменений в услугах третьей стороны	*Управление* Должен осуществляться менеджмент изменений в предоставлении услуг, включая поддержание в рабочем состоянии и улучшение существующей политики, процедур и средств управления в области защиты информации, с учетом критичности вовлеченных деловых систем и процессов и переоценки рисков.
A.10.3 Планирование и приемка систем		
Цель: Минимизировать риск системных сбоев.		
A.10.3.1	Менеджмент производитель-ности	*Управление* Использование ресурсов должно постоянно контролироваться, регулироваться, и должны делаться прогнозы будущих требований производительности, чтобы гарантировать требуемые характеристики работы системы.
A.10.3.2	Приемка системы	*Управление* Должны быть созданы критерии приемки новых информационных систем, усовершенствований и новых версий, и должны быть выполнены подходящие испытания системы(систем) в ходе разработки и перед приемкой.

A.10.4 Защита от злонамеренного и мобильного кодирования		
Цель: Защитить целостность программного обеспечения и информации.		
A.10.4.1	Средства управления, направленные против злонамеренного кодирования	*Управление* Должны быть реализованы средства управления обнаружением, предотвращением и восстановлением, имеющие целью защитить от злонамеренного кодирования, а также надлежащие процедуры [повышения] осведомленности пользователей.
A.10.4.2	Средства управления, направленные против мобильного кодирования	*Управление* Если использование мобильного кодирования разрешено, то конфигурация должна гарантировать, что разрешенное мобильное кодирование работает в соответствии с четко определенной политикой защиты, а выполнение неразрешенного мобильного кодирования должно быть предотвращено.
A.10.5 Резервное копирование		
Цель: Поддерживать целостность и доступность информации и средств, обрабатывающих информацию.		
A.10.5.1	Резервное копирование информации	*Управление* Резервные копии информации и программного обеспечения должны регулярно сниматься и проверяться в соответствии с согласованной политикой резервного копирования.
A.10.6 Менеджмент защиты сети		
Цель: Гарантировать защиту информации в сетях и защиту вспомогательной инфраструктуры.		
A.10.6.1	Средства управления сетью	*Управление* Должны осуществляться адекватный менеджмент сети и адекватное управление сетью для того, чтобы сеть была защищена от угроз и для того, чтобы поддерживать в рабочем состоянии защиту для систем и приложений, использующих сеть, включая информацию в пути.

A.10.6.2	Защита сетевых служб	*Управление* Характеристики защиты, уровни услуги, и требования менеджмента всех сетевых служб должны быть выявлены и включены в любое соглашение по сетевым услугам, независимо от того, предоставляются ли эти услуги внутренне или берутся из внешних источников.
A.10.7 Обработка носителей информации *Цель:* Предотвращать неразрешенное разглашение, изменение, удаление или уничтожение активов, а также прерывание деловых операций.		
A.10.7.1	Менеджмент съемных носителей информации	*Управление* Должны быть приняты процедуры менеджмента съемных носителей информации.
A.10.7.2	Ликвидация носителей	*Управление* Если носитель больше не требуется, то он должен быть ликвидирован надежно и безопасно, используя формальные процедуры.
A.10.7.3	Процедуры обработки информации	*Управление* Должны быть созданы процедуры для обработки и хранения информации, с целью защитить эту информацию от неразрешенного разглашения или неправильного использования.
A.10.7.4	Защита систем	*Управление* Системная документация должна быть защищена от неразрешенного доступа.
A.10.8 Обмен информацией *Цель:* Поддерживать защиту информации и программного обеспечения, выменянного в организации и в каком-либо внешнем объекте.		
A.10.8.1	Политика и процедуры обмена информацией	*Управление* Должны быть приняты официальная политика обмена, процедуры обмена и средства управления обменом, чтобы защитить обмен информации через использование всех типов средств связи.
A.10.8.2	Соглашения по обмену	*Управление* Между организацией и внешними сторонами должны быть установлены соглашения для обмена информацией и программным обеспечением.

A.10.8.3	Физические носители в процессе перемещения	*Управление* Носитель, содержащий информацию, должен быть защищен от неразрешенного доступа, неправильного использования или порчи в ходе транспортировки за физические границы организации.
A.10.8.4	Электронный обмен сообщениями	*Управление* Информация, включенная в электронный обмен сообщениями, должна быть защищена надлежащим образом.
A.10.8.5	Системы деловой информации	*Управление* Должны быть разработаны и внедрены политика и процедуры, с целью защитить информацию, связанную с взаимозависимостью систем деловой информации.
A.10.9 Услуги электронной торговли *Цель:* Гарантировать защиту услуг электронной торговли, а также их безопасное использование.		
A.10.9.1	Электронная торговля	*Управление* Информация, вовлеченная в электронную торговлю, протекающая через общедоступные сети, должна быть защищена от мошеннической деятельности, споров по договору и неразрешенного разглашения и изменения.
A.10.9.2	Сделки в режиме онлайн	*Управление* Информация, вовлеченная в сделки в режиме онлайн, должна быть защищена для того, чтобы предотвратить неполную передачу, неправильную маршрутизацию, неразрешенное изменение сообщения, неразрешенное разглашение, неразрешенное дублирование или повторное воспроизведение сообщения.
A.10.9.3	Общедоступная информация	*Управление* Целостность информации, сделанной доступной в общедоступной системе, должна быть защищена для того, чтобы предотвратить неразрешенное изменение.

A.10.10 Постоянный контроль		
Цель: Обнаруживать неразрешенную деятельность по обработке информации.		
A.10.10.1	Ведение контрольного журнала	*Управление* Контрольные журналы, записывающие деятельность пользователей, исключения и события в системе защиты информации, должны генерироваться и храниться в течение согласованного периода, с целью помочь в будущих расследованиях и в постоянном контроле над управлением доступом.
A.10.10.2	Использование систем постоянного контроля	*Управление* Должны быть созданы процедуры для постоянного контроля над использованием средств, обрабатывающих информацию, а результаты деятельности по постоянному контролю должны регулярно анализироваться.
A.10.10.3	Защита данных журнала	*Управление* Средства ведения журнала и информация журнала должны быть защищены от подделки и неразрешенного доступа.
A.10.10.4	Журнал администратора и оператора	*Управление* Деятельность системного администратора и системного оператора должны вноситься в журнал.
A.10.10.5	Журнал неисправностей	*Управление* Неисправности должны регистрироваться в журнале, анализироваться, и должно предприниматься соответствующее действие.
A.10.10.6	Синхронизация часов	*Управление* Часы всех имеющих отношение к делу систем обработки информации в пределах организации или зоны безопасности должны быть синхронизированы с согласованным источником точного времени.

A.11 Управление доступом		
A.11.1 Деловые требования к управлению доступом *Цель:* Управлять доступом к информации.		
A.11.1.1	Политика управления доступом	*Управление* На основе деловых требований и требований защиты к доступу должна быть создана, задокументирована и проанализирована политика управления доступом.
A.11.2 Менеджмент доступа пользователей *Цель:* Гарантировать доступ зарегистрированного пользователя и предотвращать неразрешенный доступ к информационным системам.		
A.11.2.1	Регистрация пользователей	*Управление* Должна быть установлена формальная процедура регистрации и снятия с регистрации пользователей, с целью предоставлять и аннулировать доступ ко всем информационным системам и услугам.
A.11.2.2	Менеджмент привилегий	*Управление* Назначение и использование привилегий должно быть ограничено, и должно управляться.
A.11.2.3	Менеджмент паролей пользователей	*Управление* Назначение паролей должно управляться через формальный процесс менеджмента.
A.11.2.4	Анализ прав доступа пользователей	*Управление* Руководство должно анализировать права доступа пользователей через регулярные интервалы, используя формальный процесс.
A.11.3 Ответственность пользователя *Цель:* Предотвращать неразрешенный доступ пользователей, а также компрометацию или кражу информации и средств, обрабатывающих информацию.		
A.11.3.1	Использование пароля	*Управление* От пользователей надо потребовать следовать хорошим методам защиты при выборе и использовании паролей.

A.11.3.2	Оборудование пользователя, работающее в автоматическом режиме	*Управление* Пользователи должны гарантировать, что оборудование, работающее в автоматическом режиме, имеет подходящую защиту.
A.11.3.3	Политика чистого стола и чистого экрана	*Управление* Должна быть принята политика чистого стола для бумаг и съемных носителей и политика чистого экрана для средств, обрабатывающих информацию.
A.11.4 Управление доступом к сети *Цель:* Предотвращать неразрешенный доступ к сетевым услугам.		
A.11.4.1	Политика по использованию сетевых услуг	*Управление* Пользователям должен предоставляться доступом только к тем услугам, которые им конкретно было разрешено использовать.
A.11.4.2	Аутентификация пользователя для внешних соединений	*Управление* Подходящие методы аутентификации должны использоваться для управления доступом дистанционных пользователей.
A.11.4.3	Идентификация оборудования в сетях	*Управление* Автоматическая идентификация оборудования должна рассматриваться как средство аутентификации соединений с конкретных мест и оборудования.
A.11.4.4	Защита удаленных диагностического и конфигурационного портов	*Управление* Физический и логический доступ к диагностическим и конфигурационным портам должен управляться.
A.11.4.5	Разделение в сетях	*Управление* Группы информационных служб, пользователей и информационные системы должны быть разделены в сетях.
A.11.4.6	Управление подключением к сети	*Управление* Для совместно эксплуатируемых сетей, особенно тех, которые простираются за границы организации, возможность пользователей по подключению к сети должна быть ограничена в соответствии с политикой управления доступом и требованиями деловых приложений (см. п.11.1).

A.11.4.7	Управление сетевой маршрутизацией	*Управление* Должны быть реализованы средства управления маршрутизацией для сетей, чтобы гарантировать, что компьютерные связи и информационные потоки не нарушают политику управления доступом деловых приложений.
A.11.5 Управление доступом к операционной системе *Цель:* Предотвращать неразрешенный доступ к операционным системам.		
A.11.5.1	Процедуры защищенного входа в систему	*Управление* Доступ к операционным системам должен управляться процедурой защищенного входа в систему.
A.11.5.2	Идентификация и аутентификация пользователя	*Управление* Все пользователи должны иметь уникальный идентификатор (ID пользователя) только для их персонального использования, и должна быть выбрана подходящая методика аутентификации для подтверждения заявленной личности пользователя.
A.11.5.3	Система менеджмента паролей	*Управление* Системы по менеджменту паролей должны быть интерактивными и должны гарантировать качественные пароли.
A.11.5.4	Использование системных утилит	*Управление* Использование утилит, которые могут быть способны блокировать средства управления системы и приложений, должны быть ограничены и должны надежно управляться.
A.11.5.5	Тайм-аут сессии	*Управление* Неактивные сеансы должны быть закрыты по истечении определенного периода бездействия.
A.11.5.6	Ограничения времени соединения	*Управление* Должны быть использованы ограничения по времени соединения, с целью обеспечить дополнительную защиту для приложений с высокой степенью риска.

A.11.6 Управление доступом к приложениям и информации		
Цель: Предотвращать неразрешенный доступ к информации, содержащейся в прикладных системах.		
A.11.6.1	Ограничение доступа к информации	*Управление* Доступ к информации и функциям прикладной системы пользователями и вспомогательным персоналом должен быть ограничен в соответствии с определенной политикой управления доступом.
A.11.6.2	Изоляция уязвимых систем	*Управление* Уязвимые системы должны иметь выделенную (изолированную) среду обработки данных.
A.11.7 Мобильная обработка и телеобработка		
Цель: Гарантировать защиту информации при использовании средств мобильной обработки и телеобработки.		
A.11.7.1	Мобильная обработка и средства связи	*Управление* Должна быть принята официальная политика и должны быть приняты надлежащие меры защиты, чтобы защититься от рисков использования средств мобильной обработки и средств связи.
A.11.7.2	Телеобработка	*Управление* Должны быть разработаны и внедрены политика, оперативные планы и процедуры для деятельности по телеобработке.
A.12 Приобретение, разработка и поддержание в рабочем состоянии информационных систем		
A.12.1 Требования защиты информационных систем		
Цель: Гарантировать, что защита является неотъемлемой частью информационных систем.		
A.12.1.1	Анализ и спецификация требований защиты	*Управление* В формулировках деловых требований для новых информационных систем или улучшений существующих информационных систем должны быть определены требования к средствам управления защитой.

A.12.2 Правильная обработка в приложениях		
Цель: Предотвращать ошибки, потерю, неразрешенное изменение или неправильное использование информации в приложениях.		
A.12.2.1	Валидация вводимых данных	*Управление* Должна осуществляться валидация данных, вводимых в приложения, с целью гарантировать, что эти данные правильные и подходящие.
A.12.2.2	Управление внутренней обработкой	*Управление* Проверки валидации должны быть включены в приложения, чтобы обнаруживать любое повреждение информации посредством обработки ошибок или сознательных действий.
A.12.2.3	Целостность сообщений	*Управление* Должны быть определены требования для обеспечения аутентичности и защиты целостности сообщений в приложениях, и должны быть определены и реализованы надлежащие средства управления.
A.12.2.4	Целостность сообщений	*Управление* Выходные данные из приложений должны быть валидированы, чтобы гарантировать, что обработка хранимой информации является правильной и подходящей обстоятельствам.
A.12.3 Управление доступом с использованием криптографии		
Цель: Защитить конфиденциальность, аутентичность или целостность информации криптографическими средствами.		
A.12.3.1	Политика по использованию криптографических символов	*Управление* Должна быть разработана и внедрена политика по использованию криптографических средств управления для защиты информации.
A.12.3.2	Распределение ключей	*Управление* Должно быть принято распределение ключей, чтобы поддерживать использование организацией методов криптографии.

A.12.4 Защита системных файлов *Цель:* Гарантировать защиту системных файлов.		
A.12.4.1	Управление системным программным обеспечением	*Управление* Должны быть приняты процедуры, чтобы управлять установкой программного обеспечения в операционных системах.
A.12.4.2	Защита данных системного теста	*Управление* Тестовые данные должны тщательно выбираться, защищаться и управляться.
A.12.4.3	Управление доступом к программе	*Управление* Доступ к исходному коду программы должен быть ограничен.
A.12.5 Защита в разработке и вспомогательных процессах *Цель:* Поддерживать защиту прикладного системного программного обеспечения и информации.		
A.12.5.1	Процедуры управления изменениями	*Управление* Реализация изменений должна управляться путем использования формальных процедур управления изменениями.
A.12.5.2	Технический анализ приложений после изменений операционной системы	*Управление* Когда операционные системы изменяются, деловые критичные приложения должны быть проанализированы и протестированы, чтобы гарантировать отсутствие неблагоприятного влияния на организационные операции или защиту.
A.12.5.3	Ограничения на изменения в пакете программ	*Управление* Изменения в пакетах программ не должны поощряться, должны быть ограничены необходимыми изменениями, и все изменения должны строго управляться.
A.12.5.4	Утечка информации	*Управление* Возможности для утечки информации должны предотвращаться.

A.12.5.5	Разработка программного обеспечения, приобретаемого на стороне	*Управление* Разработка программного обеспечения, приобретаемого на стороне, должна быть под надзором и постоянным контролем организации.
A.12.6 Менеджмент технической уязвимости *Цель:* Снизить риски, проистекающие из эксплуатации опубликованной технической уязвимости.		
A.12.6.1	Управление технической уязвимостью	*Управление* Должна получаться своевременная информация о технически уязвимых местах используемых информационных систем, должна оцениваться подверженность организации влиянию через такие уязвимые места, и должны быть предприняты подходящие меры для решения проблемы связанного с этим риска.
A.13 Менеджмент инцидентов в системе защиты информации		
A.13.1 Сообщение о событиях и слабостях в системе защиты информации *Цель:* Гарантировать, что о событиях и слабостях в системе защиты информации, связанных с информационными системами, сообщается способом, дающим возможность произвести своевременное корректирующее действие.		
A.13.1.1	Сообщение о событиях в системе защиты информации	*Управление* О событиях в системе защиты информации надо сообщать по соответствующим служебным каналам как можно быстрее.
A.13.2.2	Сообщение о слабостях в системе защиты информации	*Управление* От всех служащих, подрядчиков и сторонних пользователей информационных систем и услуг надо потребовать отмечать любые наблюдаемые или подозрительные слабости защиты в системах или услугах и сообщать о них.

A.13.2 Менеджмент инцидентов в системе защиты информации и улучшения		
Цель: Гарантировать применение последовательного и результативного подхода к менеджменту инцидентов в системе защиты информации.		
A.13.2.1	Ответственность и процедуры	*Управление* Должны быть установлены ответственность руководства и процедуры, чтобы гарантировать быструю, результативную и упорядоченную реакцию на инциденты в системе защиты информации.
A.13.2.2	Извлечение уроков из инцидентов в системе защиты информации	*Управление* Должны быть приняты механизмы для того, чтобы дать возможность определить количество типов, объемов и издержек инцидентов в системе защиты информации и постоянно их контролировать.
A.13.2.3	Сбор свидетельств	*Управление* Если последующее действие против лица или организации после инцидента в системе защиты информации включает судебный иск (или гражданский, или уголовный), то должны быть собраны, сохранены и предоставлены свидетельства, с целью соответствовать правилам для свидетельств, изложенным в соответствующей юрисдикции(юрисдикциях).
A.14 Менеджмент непрерывности бизнеса		
A.14.1 Аспекты защиты информации менеджмента непрерывности бизнеса		
Цель: Противодействовать прерываниям в деловых операциях, защитить критичные деловые процессы от влияния существенных сбоев информационных систем или бедствий, а также гарантировать своевременное возобновление деловых операций.		
A.14.1.1	Включение защиты информации в процесс менеджмента непрерывности бизнеса	*Управление* Должен быть разработан и должен поддерживаться в рабочем состоянии управляемый процесс для обеспечения непрерывности бизнеса для всей организации, который рассматривает требования защиты информации, необходимые для непрерывности бизнеса организации.

A.14.1.2	Непрерывность бизнеса и оценка риска	*Управление* Должны быть выявлены события, которые могут вызвать прерывания деловых процессов, вместе с вероятностью и негативным влиянием таких прерываний и их последствий на защиту информации.
A.14.1.3	Разработка и внедрение планов обеспечения непрерывности бизнеса, включающих защиту информации	*Управление* Должны быть разработаны и реализованы планы для поддержания в рабочем состоянии или восстановления операций и обеспечения доступности информации на требуемом уровне и в течение необходимых временных масштабов, следующих за прерыванием или сбоем в критичных деловых процессах.
A.14.1.4	Структура планирования обеспечения непрерывности бизнеса	*Управление* Должна поддерживаться в рабочем состоянии единая структура планов обеспечения непрерывности бизнеса, с целью гарантировать, что все планы согласованы, с целью последовательного обращения к требованиям защиты информации и определения приоритетов для тестирования и поддержания в рабочем состоянии.
A.14.1.5	Тестирование, постоянный контроль и переоценка планов обеспечения непрерывности бизнеса	*Управление* Планы обеспечения непрерывности бизнеса должны регулярно тестироваться и обновляться, с целью гарантировать, что они пополняются современными данными и результативны.

A.15 Соответствие

A.15.1 Соответствие законодательным требованиям

Цель: Избегать нарушений любых законодательных, уставных, нормативных или договорных обязательств, и любых требований защиты.

A.15.1.1	Выявление применимых законов	*Управление* Все имеющие отношение к делу требования закона, нормативные и договорные требования, а также способ организации выполнить эти требования должны быть четко определены, документированы и должны пополняться последними данными для каждой информационной системы и организации.

A.15.1.2	Права на интеллектуальную собственность (IPR)	*Управление* Должны быть реализованы подходящие процедуры, чтобы гарантировать соответствие законодательным, нормативным и договорным требованиям по использованию материала, в отношении которого могут иметься права на интеллектуальную собственность, и по использованию лицензионных программных продуктов.
A.15.1.3	Защита записей организации	*Управление* Важные записи должны быть защищены от потери, уничтожения и фальсификации в соответствии с требованиями закона, нормативными, договорными и деловыми требованиями.
A.15.1.4	Защита данных и секретность личной информации	*Управление* Защита данных и секретность должны гарантироваться, как требуется в соответствующем законодательстве, нормах и, если применимо, договорных статьях.
A.15.1.5	Предотвращение неправильного использования средств, обрабатывающих информацию	*Управление* Надо удерживать пользователей от использования средств, обрабатывающих информацию, для неразрешенных целей.
A.15.1.6	Регулирование средств управления доступом с использованием криптографии	*Управление* Средства управления доступом с использованием криптографии должны использоваться в соответствии со всеми соглашениями, законами и нормами, имеющими отношение к делу.
A.15.2 Соответствие политике и стандартам защиты, а также техническое соответствие *Цель:* Гарантировать соответствие систем организационной политике и стандартам защиты.		
A.15.2.1	Соответствие политике и стандартам защиты	*Управление* Менеджеры должны гарантировать, что все процедуры защиты в пределах их зоны ответственности выполняются правильно, с целью достичь соответствия политике и стандартам защиты.

A.15.2.2	Проверка технического соответствия	*Управление* Информационные системы должны регулярно проверяться на соответствие стандартам реализации защиты.
A.15.3 Обдумывание аудита информационных систем *Цель:* Максимизировать результативность и минимизировать помехи для/от процесса аудита информационных систем.		
A.15.3.1	Средства управления аудитом информационных систем	*Управление* Требования аудита и деятельность по аудиту, включающая проверки в действующих системах, должны быть тщательно спланированы и согласованы, с целью минимизировать риск срыва деловых процессов.
A.15.3.2	Защита информации	*Управление* Доступ к инструментальным средствам аудита информационных систем должен быть защищен, чтобы предотвратить любое возможное неправильное употребление или компрометацию.

Приложение B
(информационное)

Принципы OECD[6] и этот международный стандарт

Принципы, приведенные в Руководящих указаниях OECD по защите информационных систем и сетей, относятся ко всей политике и оперативным уровням, которые управляют защитой информационных систем и сетей. В этом международном стандарте представлена структура системы менеджмента защиты информации для реализации некоторых принципов OECD, использующих модель PDCA, и процессы, описанные в Разделах 4, 5, 6 и 8, как указано в таблице B.1.

Таблица B.1 — Принципы QECD и модель PDCA

Принципы QECD	**Соответствующий процесс СМЗИ и фаза PDCA**
Осведомленность Участникам следует быть осведомленными о потребности в защите информационных систем и сетей и о том, что они могут сделать для улучшения защиты.	Эта деятельность является частью фазы **Осуществление** (см. п.4.2.2 и **п.5.2.2**).
Ответственность Все участники несут ответственность за защиту информационных систем и сетей.	Эта деятельность является частью фазы **Осуществление** (см. п.4.2.2 и **п.5.1**).
Реакция Участникам следует действовать своевременно и совместно, чтобы предотвращать, обнаруживать и реагировать на инциденты в системе защиты информации.	Это часть деятельности по постоянному контролю фазы **Проверка** (см. п.4.2.3 и пп.6—7.3) и реагирующей деятельности фазы **Действие** (см. п.4.2.4 и пп.8.1—8.3). Это также может быть охвачено некоторыми аспектами фаз **Планирование** и **Проверка**.
Оценка риска Участникам следует проводить оценки рисков.	Эта деятельность является частью фазы **Планирование** (см. п.4.2.1), а переоценка риска является частью фазы **Проверка** (см. п.4.2.3 и пп.6—7.3).

[6] OECD (*сокр. от* Organization for Economic Co-operation and Development) — Организация экономического сотрудничества и развития (*Прим. переводчика*)

Проектирование и реализация защиты Участникам следует включить защиту как существенный элемент информационных систем и сетей.	Как только оценка риска завершена, выбираются средства управления для обработки рисков как часть фазы **Планирование** (см. п.4.2.1). Тогда фаза **Осуществление** (см. п.4.2.2 и п.5.2) охватывает реализацию и эксплуатацию этих средств управления.
Менеджмент защиты Участникам следует принять комплексный подход к менеджменту защиты.	Управление риска является процессом, который включает предотвращение, обнаружение и реакцию на инциденты, ведущееся поддержание в рабочем состоянии, анализ и аудит. Все эти аспекты охвачены в фазах **Планирование**, **Осуществление**, **Проверка** и **Действие**.
Переоценка Участникам следует анализировать и переоценивать защиту информационных систем и сетей и делать надлежащие изменения в политике, методах, мерах и процедурах защиты.	Переоценка защиты информации является частью фазы **Проверка** (см. п.4.2.3 и пп.6—7.3), где следует проводить регулярный анализ, с целью проверять результативность системы менеджмента защиты информации, а улучшение защиты является частью фазы **Действие** (см. п.4.2.4 и пп.8.1—8.3).

Приложение C
(информационное)

Соответствие между ISO 9001:2000, ISO 14001:2004 и этим международным стандартом

В таблице C.1 показано соответствие между ISO 9001:2000, ISO 14001:2004 и этим международным стандартом.

Таблица C.1 — Соответствие между ISO 9001:2000, ISO 14001:2004 и этим международным стандартом

Этот международный стандарт	**ISO 9001:2000**	**ISO 14001:2004**
0 Введение	**0 Введение**	**Введение**
0.1 Общие положения	0.1 Общие положения	
0.2 Процессный подход	0.2 Процессный подход	
	0.3 Связь с ИСО 9004	
0.3 Совместимость с другими системами менеджмента	0.4 Совместимость с другими системами менеджмента	
1 Область приложения	**1 Область приложения**	**1 Область приложения**
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 Системы менеджмента защиты информации	**4 Система менеджмента качества**	**4 Требования EMS[7]**
4.1 Общие требования	4.1 Общие требования	4.1 Общие требования
4.2 Создание и менеджмент СМЗИ		
4.2.1 Создать СМЗИ		

[7] EMS (сокр. от Ecological management system) — Система экологического менеджмента (*Прим. переводчика*)

Этот международный стандарт	ISO 9001:2000	ISO 14001:2004
4.2.2 Реализовать и эксплуатировать СМЗИ		4.4 Реализация и эксплуатация
4.2.3 Постоянно контролировать и анализировать СМЗИ	8.2.3 Постоянный контроль и измерение процессов	4.5.1 Постоянный контроль и измерение
	8.2.4 Постоянный контроль и измерение продукции	
4.2.4 Поддерживать в рабочем состоянии и улучшать СМЗИ		
4.3 Требования к документации	4.2 Требования к документации	
4.3.1 Общие положения	4.2.1 Общие положения	
4.3.2 Управление документами	4.2.3 Управление документами	4.4.5 Управление документами
4.3.3 Управление записями	4.3.4 Управление записями	4.5.4 Управление записями
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	5.3 Политика в области защиты окружающей среды
	5.4 Планирование	4.3 Планирование
	5.4 Ответственность, полномочия и обмен информацией	

Этот международный стандарт	**ISO 9001:2000**	**ISO 14001:2004**
5.2 Менеджмент ресурсов	**6 Менеджмент ресурсов**	
5.2.1 Обеспечение ресурсами	6.1 Обеспечение ресурсами	
	6.2 Человеческие ресурсы	
5.2.2 Подготовка, осведомленность и компетентность	6.2.2 Компетентность, осведомленность и подготовка	4.4.2 Компетентность, подготовка и осведомленность
	6.3 Инфраструктура	
	6.4 Производственная среда	
6 Внутренние аудиты СМЗИ	8.2.2 Внутренний аудит	4.5.5 Внутренний аудит
7 Анализ СМЗИ со стороны руководства	**5.6 Анализ со стороны руководства**	**4.6 Анализ со стороны руководства**
7.1 Общие положения	5.6.1 Общие положения	
7.2 Входные данные для анализа	5.6.2 Входные данные для анализа	
7.3 Выходные данные анализа	5.6.3 Выходные данные анализа	
8 Улучшение СМЗИ	**8.5 Улучшение**	
8.1 Постоянное улучшение	8.5.1 Постоянное улучшение	
8.2 Корректирующие действия	8.5.2 Корректирующие действия	
8.3 Предупреждающие действия	8.5.3 Предупреждающие действия	

Этот международный стандарт	ISO 9001:2000	ISO 14001:2004
Приложение A Цели управления и средства управления		Приложение A Руководящие указания по использованию данного международного стандарта
Приложение B Принципы OECD и этот международный стандарт		
Приложение C Соответствие между ISO 9001:2000, ISO 14001:2004 и этим международным стандартом	Приложение A Соответствие между ISO 9001:2000 и ISO 14001:1996	Приложение B Соответствие между ISO 14001:2004 и ISO 9001:2000

Библиография

Публикации стандартов

[1] ISO 9001:2000*, Quality management systems — Requirements*

[2] ISO/IEC 13335-1:2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

[3] ISO/IEC TR 13335-3:1998, *Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security*

[4] ISO/IEC TR 13335-4:2000, *Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards*

[5] ISO 14001:2004, *Environmental management systems — Requirements with guidance for use*

[6] ISO/IEC TR 18044:2004, *Information technology — Security techniques — Information security incident management*

[7] ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*

[8] ISO/IEC Guide 62:1996, *General requirements for bodies operating assessment and certification/registration of quality systems*

[9] ISO/IEC Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards*

Другие публикации

[1] OECD, *Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org*

[2] NIST SP 800-30, *Risk Management Guide for Information Technology Systems*

[3] Deming W.E., Out *of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 1986*