

---

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

*Technologies de l'information — Techniques de securite — Systemes  
de gestion de securite de l'information — Exigences*

---

Технологии информационные. Методы  
обеспечения защиты. Системы управления  
информации. Требования

---

---

Reference number  
ISO/IEC 27001:2005(E)



# Содержание

<b>0 ВВЕДЕНИЕ</b> .....	<b>4</b>
<b>1 ОБЗОР</b> .....	<b>6</b>
1.1 Общие положения.....	6
1.2 Применение.....	6
<b>2 НОРМАТИВНЫЕ ССЫЛКИ</b> .....	<b>7</b>
<b>3 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ</b> .....	<b>7</b>
<b>4 СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b> .....	<b>9</b>
4.1 Общие требования.....	9
4.2 Создание и менеджмент СМИБ.....	9
4.3 Требования обеспечения документацией .....	12
<b>5 ОБЯЗАННОСТИ РУКОВОДСТВА</b> .....	<b>14</b>
5.1 Обязательства руководства.....	14
5.2 Управление трудовыми ресурсами .....	14
<b>6 ВНУТРЕННИЕ АУДИТЫ СМИБ</b> .....	<b>14</b>
<b>7 ПРОВЕРКА УПРАВЛЕНИЯ СМИБ</b> .....	<b>15</b>
7.1 Общие положения.....	15
7.2 Входные данные для проверки.....	15
7.3 Выходные данные проверки .....	16
<b>8 СОВЕРШЕНСТВОВАНИЕ СМИБ</b> .....	<b>16</b>
8.1 Постоянное совершенствование .....	16
8.2 Корректирующие меры .....	16
8.3 Превентивные мероприятия .....	16
ПРИЛОЖЕНИЕ А.....	18
ПРИЛОЖЕНИЕ В.....	30
ПРИЛОЖЕНИЕ С.....	31
<b>БИБЛИОГРАФИЯ</b> .....	<b>33</b>

### Предисловие

МОС (Международная организация по стандартизации) и МЭК (Международная электротехническая комиссия) формируют специализированную систему стандартизации, распространённую во всём мире. Национальные организации, являющиеся членами МОС и МЭК, участвуют в развитии Международных Стандартов посредством технических комиссий, учреждённых соответствующей организацией, чтобы работать с особыми сферами технической деятельности. Технические комиссии МОС и МЭК сотрудничают в сферах взаимного интереса. Другие международные организации, государственные либо негосударственные, совместно с МОС и МЭК также участвуют в работе. В сфере информационных технологий МОС и МЭК учредили совместную комиссию, МОС/МЭК ОТК.

Международные Стандарты проектируются в соответствии с правилами, описанными в Положениях МОС/МЭК, Часть 2.

Главная задача объединённой технической комиссии состоит в подготовке Международных Стандартов. Проекты Международных Стандартов, принимаемые объединённой технической комиссией, передаются национальным комиссиям на рассмотрение и голосование. Для издания Международных Стандартов необходимо набрать 75% голосов национальных организаций.

Особое внимание привлекает вероятность того, что некоторые элементы данного документа могут быть запатентованы. МОС и МЭК не несут ответственность за определение некоторых или всех таких патентов.

Стандарт МОС/МЭК 27001 был подготовлен Объединённой Электротехнической Комиссией МОС/МЭК ОТК 1, *Информационные технологии*, Подкомиссия ПК 27, *Способы защиты ИТ*.

## 0 Введение

### 0.1 Общие положения

Данный Международный Стандарт разработан для создания модели по созданию, внедрению, использованию, мониторингу, проверке, поддержке и совершенствованию Системы Менеджмента Информационной Безопасности (СМИБ). Утверждение СМИБ должно стать стратегическим решением для организации. Проектирование и внедрение СМИБ в организации зависит от её нужд и целей, требований безопасности, применяющихся процессов (технологических приёмов), а также её размера и структуры. Предполагается, что со временем такие системы, а также их поддерживающие, изменятся. Полагают, что внедрение СМИБ будет проводиться по определённой шкале в соответствии с нуждами организации, например, простая ситуация требует и простого решения СМИБ.

Данный Международный Стандарт может быть использован заинтересованными внутренней и внешней сторонами для определения соответствия системы нормам безопасности.

### 0.2 Концепция процесса менеджмента

Данный Международный Стандарт утверждает концепцию процесса создания, внедрения, использования, мониторинга, проверки, поддержки и совершенствования СМИБ организации.

Для эффективного функционирования организации приходится идентифицировать и управлять многими процессами. Процессом может считаться любое действие, использующее ресурсы, и управляемое в целях преобразования входных данных в выходные. Зачастую результат одного процесса обращается непосредственно во входной сигнал другого.

Применение системы процессов в рамках организации наряду с идентификацией и взаимодействием этих процессов, их менеджментом, можно рассматривать как “концепцию процесса”.

Представленная в данном Международном Стандарте концепция процесса менеджмента информационной безопасности заставляет тех, кто её использует, задуматься о важности таких моментов, как:

- а) понимание требований информационной безопасности организации и необходимости проводить политику и устанавливать цели информационной безопасности;
- б) введение директив по внедрению и эксплуатации для управления рисками информационной безопасности организации в контексте суммарных бизнес-рисков организации;
- в) мониторинг и проверка качества функционирования и эффективности СМИБ; а также
- г) постоянное совершенствование, основанное на реальных оценках.

Данный Международный Стандарт утверждает модель “Планируй-Делай-Проверяй-Действуй” (PDCA), которая призвана структурировать все процессы СМИБ. Рисунок 1 иллюстрирует как в СМИБ поступающие на вход требования и ожидания безопасности заинтересованных сторон, проходя все необходимые операции и процессы, превращаются на выходе в информационную безопасность, отвечающую этим требованиям и ожиданиям. Также на Рисунке 1 изображены связи процессов, представленных в параграфах 4,5,6,7и 8.

Утверждение модели PDCA также может отразить принципы, изложенные в директивах ОЭСР (2002) по управлению безопасностью информационных систем и сетей. Данный Международный Стандарт предоставляет прочную модель внедрения правил в инструкции по управлению оценкой рисков, моделированием и обеспечением безопасности, менеджментом и переоценкой безопасности.

#### ПРИМЕР 1

Требование может быть таким: нарушения в информационной безопасности, которые не приведут к серьёзному финансовому ущербу организации и/или только доставят организации некоторые трудности.

#### ПРИМЕР 2

Ожидание может быть такое: на случай происшествия серьёзного инцидента – возможно атака на веб-сайт, через который организация осуществляет Интернет-бизнес, – должны быть сотрудники, достаточно квалифицированные для проведения соответствующих мероприятий в целях минимизации воздействия атаки.

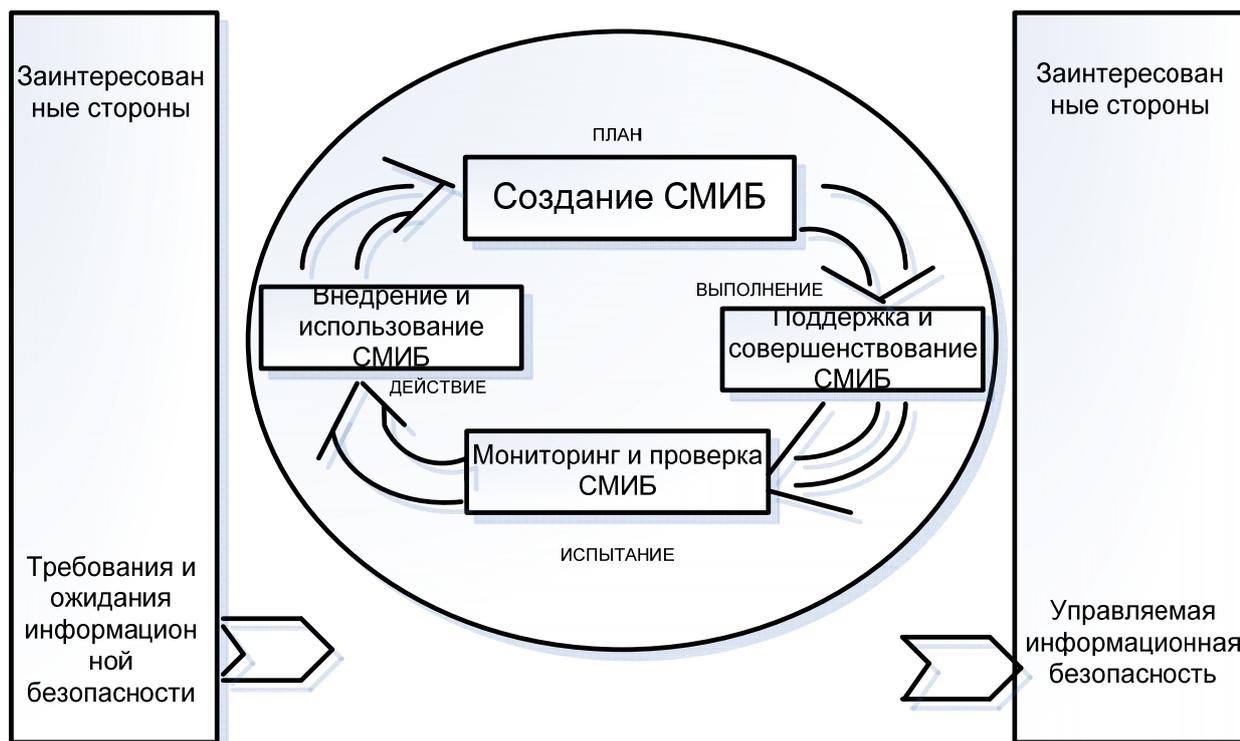


Рисунок 1 Применение модели PDCA в процессах СМИБ

<b>Планирование (создание СМИБ)</b>	Введение политики, установление целей, процессов и процедур, относящихся к управлению риском и совершенствованию информационной безопасности для достижения результатов в соответствии с политиками и целями организации.
<b>Осуществление (внедрение и использование СМИБ)</b>	Внедрение и использование политик, директив, процессов и мероприятий СМИБ.
<b>Испытание (мониторинг и проверка СМИБ)</b>	Оценка, а где возможно, и измерение эксплуатационных характеристик процессов в соответствии с политикой, целями СМИБ и практическим опытом, отчёт по полученным результатам для проверки.
<b>Выполнение (поддержка и совершенствование СМИБ)</b>	Проведение корректирующих и превентивных мероприятий, основанных на результатах внутреннего аудита СМИБ и проверки или другой значимой информации, в целях достижения постоянного совершенствования СМИБ.

### 0.3 Совместимость с другими системами менеджмента

В целях обеспечения совместимого и комплексного внедрения и использования данного Международного Стандарта с родственными ему стандартами менеджмента, такими, как ISO 9001:2000 и ISO 14001:2004, его разработка велась в соответствии с принципами и определениями вышеперечисленных стандартов. Потому одна надлежащим образом разработанная система менеджмента может удовлетворять требованиям всех этих стандартов. В таблице С.1 изображена связь между параграфами данного Международного Стандарта, стандартов ISO 9001:2000 и ISO 14001:2004.

Цель данного Международного Стандарта – позволить организации урегулировать либо интегрировать свою СМИБ с соответствующими требованиями систем менеджмента.

# Информационные технологии — Концепции безопасности — Системы менеджмента информационной безопасности — Требования

**ВАЖНО** — Данное издание не подразумевает включение всех требуемых положений документа. Только пользователи ответственны за их корректное применение. Само по себе соответствие Международному Стандарту не освобождает от правовых обязательств.

## 1 Обзор

### 1.1 Общие положения

Данный Международный Стандарт охватывает все виды организаций (например, коммерческие структуры, правительственные учреждения, некоммерческие предприятия)

Данный Международный Стандарт определяет требования для создания, внедрения, использования, мониторинга, проверки, поддержки и совершенствования документированной СМИБ в контексте суммарного количества бизнес-рисков организации. Он определяет требования для внедрения средств обеспечения защиты, переделанных под нужды отдельных организаций и их частей.

Цель разработки СМИБ – обеспечить отбор только отвечающих требованиям и соразмерных средств обеспечения безопасности, способных защитить информационные активы и предоставить уверенность в безопасности заинтересованным лицам.

**ПРИМЕЧАНИЕ 1:** Понятие “бизнеса” в данном Международном Стандарте следует интерпретировать в широком смысле для обозначения деятельности, необходимой для существования организации.

**ПРИМЕЧАНИЕ 2:** МОС/МЭК 17799 предоставляет руководство по обеспечению безопасности, которое можно использовать для разработки директив.

### 1.2 Применение

Требования, представленные в данном Международном Стандарте, являются общими и применимы ко всем организациям, независимо от их вида, размера и характера деятельности. Исключение любых требований, определённых в параграфах 4, 5, 6, 7 и 8 недопустимо, если организация предъявляет требования соответствия данному Международному Стандарту.

Любое исключение директив, необходимое, чтобы соответствовать критерию принятия риска, должно быть обосновано, и также должны быть предъявлены доказательства о принятии ответственными лицами связанных с этим рисков. В тех случаях, когда какие-либо пункты исключаются, претензии к согласованности с данным Международным Стандартом не принимаются до тех пор, пока подобные исключения ради обеспечения информационной безопасности, отвечающей требованиям безопасности, определённым оценкой рисков, и соответствующим юридическим и регулятивным требованиям, не влияют на производительность организации и/или обязательства.

**ПРИМЕЧАНИЕ:** Если в организации уже действует оперативная система менеджмента бизнес-процессами (например, в соответствии со стандартами МОС 9001 или МОС1 4001), в большинстве случаев будет предпочтительнее удовлетворять требованиям этого международного стандарта в рамках этой существующей системы менеджмента.

## 2 Нормативные ссылки

Следующие нормативно-справочные документы обязательны в качестве приложения к этому документу. Для датированных ссылок применимо только упомянутое издание. Для недатированных ссылок применимо последнее издание нормативно-справочного материала (включая поправки).

*МОС/МЭК 17799:2005, Информационные технологии – Методы обеспечения защиты – Свод правил практического применения менеджмента информационной безопасности.*

## 3 Термины и определения

В данном документе используются следующие термины и определения.

### 3.1

#### **ценные активы**

всё, что имеет ценность для организации

[МОС/МЭК 13335-1:2004]

### 3.2

#### **доступность**

свойство быть доступным и используемым по требованию авторизованного субъекта

[МОС/МЭК 13335-1:2004]

### 3.3

#### **конфиденциальность**

свойство, обеспечивающее недоступность и закрытость информации для неавторизованных индивидов, субъектов или процессов

[МОС/МЭК 13335-1:2004]

### 3.4

#### **информационная безопасность**

обеспечение конфиденциальности, целостности и доступности информации; также возможно обеспечение и других свойств, таких как аутентичность, идентифицируемость, отказоустойчивость и надёжность.

[МОС/МЭК 17799:2005]

### 3.5

#### **событие в информационной безопасности**

установленное происшествие (эпизод) в системе, службе или сети, свидетельствующее о возможной бреши в политике информационной безопасности или отсутствии мер безопасности, или же о до этого неизвестном случае, возможно имеющем отношение к безопасности

[МОС/МЭК ТУ 18044:2004]

### 3.6

#### **инцидент в информационной безопасности**

единичное событие или же ряд нежелательных или неожиданных событий в информационной безопасности, которые подвергают большому риску бизнес-процессы или же угрожают информационной безопасности

[МОС/МЭК ТУ 18044:2004]

### 3.7

#### **система менеджмента информационной безопасности**

#### **СМИБ**

это часть комплексной системы менеджмента, основанная на концепции бизнес-рисков, предназначена для создания, внедрения, использования, мониторинга, проверки, поддержки и совершенствования информационной безопасности

ПРИМЕЧАНИЕ: Система менеджмента включает организационную структуру, политики безопасности, мероприятия по планированию управления, обязательства, инструкции, методики проведения, процедуры и ресурсы

### **3.8**

#### **целостность**

свойство сохранения точности и полноты активов

[МОС/МЭК 13335-1:2004]

### **3.9**

#### **остаточный риск**

риск, остающийся после сокращения риска

[МОС/МЭК Руководство 73:2002]

### **3.10**

#### **принятие риска**

решения принять риск

[МОС/МЭК Руководство 73:2002]

### **3.11**

#### **анализ рисков**

систематическое использование информации для определения источников риска и оценки рисков

[МОС/МЭК Руководство 73:2002]

### **3.12**

#### **оценка рисков**

процесс, охватывающий и анализ рисков, и оценку рисков

[МОС/МЭК Руководство 73:2002]

### **3.13**

#### **оценивание риска**

процесс сравнения оцененного риска с данными критериями риска для определения значимости риска.

[МОС/МЭК Руководство 73:2002]

### **3.14**

#### **управление рисками**

согласованные действия по руководству и управлению организацией в отношении риска

[МОС/МЭК Руководство 73:2002]

### **3.15**

#### **сокращение риска**

процесс отбора и проведения мероприятий по изменению риска

[МОС/МЭК Руководство 73:2002]

ПРИМЕЧАНИЕ: В данном международном стандарте термин «управление» употребляется как синоним к термину «мера».

### **3.16**

#### **предписание по применимости**

документированное положение, описывающее цели и средства управления, уместные и применимые в СМИБ организации

ПРИМЕЧАНИЕ: Цели и выбор средств управления основаны на результатах и выводах процессов оценки и сокращения рисков, юридических или регулятивных требованиях, договорных обязательствах и требованиях касательно бизнеса организации в целях обеспечения информационной безопасности.

## 4 Система менеджмента информационной безопасности

### 4.1 Общие требования

Организация должна вводить, выполнять, использовать, контролировать, пересматривать, поддерживать и совершенствовать документированные положения СМИБ в рамках всей бизнес-деятельности организации, а также рисков, с которыми она сталкивается. Ради практической пользы данного Международного Стандарта используемый процесс основывается на модели PDCA, показанной на рис. 1.

### 4.2 Создание и менеджмент СМИБ

#### 4.2.1 Создание СМИБ

Организация должна сделать следующее.

а) Учитывая особенности деятельности организации, самой организации, ее месторасположения, активов и технологии, определить масштаб и границы СМИБ, включая детали и обоснования исключений каких-либо положений документа из проекта СМИБ (см.1.2).

б) Учитывая особенности деятельности организации, самой организации, ее месторасположения, активов и технологии, разработать политику СМИБ которая:

- 1) включает систему постановки целей (задач) и устанавливает общее направление руководства и принципы действия относительно информационной безопасности;
- 2) принимает во внимание деловые и юридические или регулятивные требования, договорные обязательства по безопасности;
- 3) присоединена к стратегической среде управления риском, в которой имеет место создание и поддержка СМИБ;
- 4) устанавливает критерии, по которым будет оцениваться риск (см. 4.2.1 с)); и
- 5) утверждена руководством.

ПРИМЕЧАНИЕ: В целях этого Международного Стандарта, политикой СМИБ считается расширенный набор политик информационной безопасности. Эти политики могут быть описаны в одном документе.

с) Разработать концепцию оценки риска в организации.

- 1) Определить методологию оценки риска, которая подходит СМИБ, и установленной деловой информационной безопасности, юридическим и регулятивным требованиям.
- 2) Разрабатывать критерии принятия риска и определять приемлемые уровни риска (см. 5.1f). Выбранная методология оценки риска должна гарантировать, что оценка риска приносит сравнимые и воспроизводимые результаты.

ПРИМЕЧАНИЕ: Существуют различные методологии оценки риска. Примеры методологий оценки риска рассмотрены в МОС/МЭК ТУ 13335-3, *Информационные технологии – Рекомендации к менеджменту ИТ Безопасности – Методы менеджмента ИТ Безопасности*.

d) Выявить риски.

- 1) Определить активы в рамках положений СМИБ, и владельцев<sup>2</sup> (<sup>2</sup> Термин «владелец» отождествляется с индивидуом или субъектом, которая утверждена нести ответственность за контроль производства, развития, технического обслуживания, применения и безопасности активов. Термин «владелец» не означает, что персона действительно имеет какие-либо права собственности на актив) этих активов.

- 2) Выявить опасности для этих активов.
- 3) Выявить уязвимые места в системе защиты.
- 4) Выявить воздействия, которые разрушают конфиденциальность, целостность и доступность активов.

е) Проанализировать и оценить риски.

- 1) Оценить ущерб бизнесу организации, который может быть нанесён вследствие несостоятельности системы защиты, а также являться последствием нарушения конфиденциальности, целостности, или доступности активов.
- 2) Определить вероятность провала системы безопасности в свете преобладающих опасностей и уязвимостей, ударов, связанных с активами, и внедренных в настоящее время элементов управления.
- 3) Оценить уровни риска.
- 4) Определить приемлемость риска, или же требовать его сокращения, используя критерии допустимости риска, установленные в 4.2.1с)2).

ф) Выявить и оценить инструменты для сокращения риска.

Возможные действия включают:

- 1) Применение подходящих элементов управления;
- 2) Сознательное и объективное принятие рисков, гарантирующее их безусловное соответствие требованиям политики организации и критериям допустимости риска (см. 4.2.1с)2));
- 3) Избежание риска; и
- 4) Передача соответствующих бизнес-рисков другой стороне, например, страховым компаниям, поставщикам.

г) Выбрать задачи и средства управления для сокращения рисков.

Задачи и средства управления должны быть выбраны и внедрены в соответствии с требованиями, установленными процессом оценкой риска и сокращения риска. Этот выбор должен учитывать как критерии допустимости риска (см. 4.2.1с)2)), так и юридические, регулятивные и договорные требования.

Задачи и средства управления из Приложения А должны быть выбраны как часть этого процесса, отвечающие установленным требованиям.

Т.к. в Приложении А перечислены не все задачи и средства управления, то могут быть выбраны дополнительные.

**ПРИМЕЧАНИЕ:** Приложение А содержит всесторонний список целей управления, которые были определены как наиболее значимые для организаций. Чтобы не пропустить ни один важный пункт из опций управления, пользующимся данным Международным Стандартом следует ориентироваться на Приложение А как на отправной пункт для контроля выборки.

h) Достигнуть утверждения управления предполагаемыми остаточными рисками.

i) Достигнуть авторизации управления для функционирования СМИБ.

j) Составить Декларацию Применимости

А Декларация Применимости должна включать следующее:

- 1) задачи и средства управления, выбранные в 4.2.1г), и причины их выбора;

- 2) задачи и средства управления, действующие в настоящее время (см. 4.2.1e)2)); и
- 3) исключение каких-либо задач и средств управления из Приложения А и обоснование их исключения.

**ПРИМЕЧАНИЕ:** Декларация применимости представляет собой сводку решений относительно сокращения риска. Обоснование исключений обеспечивает перепроверку по разным источникам того, что ни одного элемента управления не было упущено.

#### 4.2.2 Внедрение и использование СМИБ

Организация должна сделать следующее.

- a) Сформулировать план сокращения риска, который определяет соответствующие управляющие действия, ресурсы, обязательства и приоритеты для управления рисками информационной безопасности (см. 5).
- b) Осуществить план сокращения рисков для того, чтобы достигнуть установленных целей, которые включают анализ финансирования и распределения ролей и обязанностей.
- c) Внедрить средства управления, выбранные в 4.2.1g), для достижения поставленных целей.
- d) Определить, как измерить эффективность выбранных средств управления или групп средств управления, и установить как эта система мер должна использоваться, чтобы оценить эффективность управления и получить соизмеримые и воспроизводимые результаты (см. 4.2.3c)).

**ПРИМЕЧАНИЕ:** Оценка эффективности средств управления позволяет менеджерам и штату служащих определить, насколько хорошо средства управления достигают поставленных целей.

- e) Внедрить обучающие и информирующие программы (см. 5.2.2).
- f) Управлять функционированием СМИБ.
- g) Обеспечить СМИБ трудовыми ресурсами (см. 5.2)
- h) Внедрить методику и другие средства управления, способные своевременно выявить события безопасности и ответную реакцию на инциденты безопасности (см. 4.2.3a)).

#### 4.2.3 Мониторинг и проверка СМИБ

Организация должна сделать следующее.

- a) Внедрить правила мониторинга и проверки и другие средства управления для того, чтобы:
  - 1) своевременно обнаруживать ошибки в результатах процесса;
  - 2) своевременно распознавать неудавшиеся и удавшиеся нарушения безопасности и инциденты;
  - 3) задействовать менеджмент, чтобы определить, надлежащим ли образом выполняется работа по безопасности, порученная людям либо осуществляемая информационными технологиями;
  - 4) содействовать обнаружению событий безопасности и таким образом, используя определённые показатели, предупреждать инциденты безопасности; и
  - 5) определить эффективность действий, предпринятых для предотвращения нарушения безопасности.
- b) Проводить регулярные проверки эффективности СМИБ (включая обсуждение политики СМИБ и её задач, проверку средств управления безопасностью), принимая во внимание результаты аудитов, инцидентов, результаты измерений эффективности, предложения и

рекомендации всех заинтересованных сторон.

с) Оценить эффективность средств управления, чтобы выявить, удовлетворены ли требования безопасности.

д) Проверить оценку рисков по запланированным периодам и проверить остаточные риски и допустимые уровни рисков, принимая во внимания изменения в:

- 1) организации;
- 2) технологии;
- 3) бизнес-целях и процессах;
- 4) идентифицированных угрозах;
- 5) эффективности внедрённых средств управления; и
- 6) внешних событиях, таких как изменения в юридической и управленческой среде, изменённые договорные обязательства, смены социального климата.

е) Проводить внутренние аудиты СМИБ в запланированные периоды (см. 6)

ПРИМЕЧАНИЕ: Внутренние аудиты, иногда называемые первичными аудитами, проводятся от имени самой организации в её собственных целях.

ф) На регулярной основе проводить проверку управления СМИБ, чтобы убедиться, что положение остается пригодным, а СМИБ совершенствуется.

г) Обновлять планы безопасности с учётом данных, полученных в результате мониторинга и проверки.

h) Записывать действия и события, которые могут оказать влияние на эффективность или производительность СМИБ (см. 4.3.3).

#### **4.2.4 Поддержка и совершенствование СМИБ**

Организация должна постоянно делать следующее.

- а) Внедрять в СМИБ определённые исправления.
- б) Предпринимать соответствующие корректирующие и превентивные меры в соответствии с 8.2 и 8.3. Применять знания, накопленные самой организацией и полученные из опыта других организаций.
- с) Сообщать о своих действиях и совершенствованиях всем заинтересованным сторонам в степени детализации, соответствующей обстановке; и, соответственно, согласовывать свои действия.
- д) Убедиться, что улучшения достигли намеченной цели.

### **4.3 Требования обеспечения документацией**

#### **4.3.1 Общие положения**

Документация должна включать протоколы (записи) управленческих решений, убеждать в том, что необходимость действий обусловлена решениями и политикой менеджмента; и убеждать во воспроизводимости записанных результатов.

Важно уметь демонстрировать обратную связь выбранных средств управления с результатами процессов оценки риска и его сокращения, и далее с политикой СМИБ и ее целями.

В документацию СМИБ необходимо включить:

- a) документированные формулировки политики и целей СМИБ (см. 4.2.1b));
- b) положение СМИБ (см. 4.2.1a));
- c) концепцию и средства управления в поддержку СМИБ;
- d) описание методологии оценки риска (см. 4.2.1c));
- e) отчет об оценке риска (см. 4.2.1c) – 4.2.1g));
- f) план сокращения риска (см. 4.2.2b));
- g) документированную концепцию, необходимую организации для обеспечения эффективности планирования, функционирования и управления процессами её информационной безопасности и описания способов измерения эффективности средств управления (см. 4.2.3c));
- h) документы, требуемые данным Международным Стандартом (см. 4.3.3); и
- i) Утверждение о Применимости.

ПРИМЕЧАНИЕ 1: В рамках данного Международного Стандарта термин «документированная концепция» означает, что концепция внедрена, документирована, выполняется и соблюдается.

ПРИМЕЧАНИЕ 2: Размер документации СМИБ в различных организациях может колебаться в зависимости от:

- размера организации и типа ее активов; и
- масштаба и сложности требований безопасности и управляемой системы.

ПРИМЕЧАНИЕ 3: Документы и отчёты могут предоставляться в любой форме.

#### 4.3.2 Контроль документов

Документы, требуемые СМИБ, необходимо защищать и регулировать. Необходимо утвердить процедуру документации, необходимую для описания управленческих действий по:

- a) установлению соответствия документов определённым нормам до их опубликования;
- b) проверке и обновлению документов как необходимости, переутверждению документов;
- c) обеспечению соответствия изменений текущему состоянию исправленных документов;
- d) обеспечению доступности важных версий действующих документов;
- e) обеспечению понятности и читабельности документов;
- f) обеспечению доступности документов тем, кому они необходимы; а также их передачи, хранения и, наконец, уничтожения в соответствии с процедурами, применяемыми в зависимости от их классификации;
- g) установлению подлинности документов из внешних источников;
- h) контролированию распространения документов;
- i) предупреждению непреднамеренного использования вышедших из употребления документов;
- и
- j) применению к ним соответствующего способа идентификации, если они хранятся просто на всякий случай.

#### 4.3.3 Контроль записей

Записи должны создаваться и храниться для того, чтобы обеспечить подтверждение соответствия требованиям и эффективное функционирование СМИБ. Записи необходимо защищать и проверять. СМИБ должна учитывать любые юридические и регулятивные требования и договорные обязательства. Записи должны быть понятны, легко идентифицируемы и восстанавливаемы. Средства управления, необходимые для идентификации, хранения, защиты, восстановления, продолжительности хранения и уничтожения записей, должны быть документально утверждены и введены в действие.

В записи необходимо включать информацию о проведении мероприятий, описанных в 4.2, и обо всех происшествиях и значимых для безопасности инцидентах, относящихся к СМИБ.

#### ПРИМЕР

Примерами записей являются гостевая книга, протоколы аудита и заполненные формы авторизации доступа.

## **5 Обязанности руководства**

### **5.1 Обязательства руководства**

Руководство должно подтвердить свои обязательства по введению, реализации, функционированию, мониторингу, проверке, поддержке и совершенствованию СМИБ путем:

- a) введения политики СМИБ;
- b) постановки целей СМИБ и разработки планов;
- c) распределения ролей и обязанностей в информационной безопасности;
- d) донесения до организации важности выполнения задач по информационной безопасности, согласования их с политикой безопасности, ответственностью в соответствии с законом, и необходимости постоянного совершенствования;
- e) достаточного обеспечения трудовыми ресурсами, чтобы ввести, реализовать, управлять, наблюдать, проверять, поддерживать и совершенствовать СМИБ (см. 5.2.1);
- f) установления критериев принятия риска и допустимых уровней риска;
- g) проведения внутренних аудитов СМИБ (см. 6); и
- h) проведения проверок управления СМИБ (см. 7).

### **5.2 Управление трудовыми ресурсами**

#### **5.2.1 Обеспечение кадрами**

Организация должна определить и подобрать штат сотрудников, необходимых для того, чтобы:

- a) создавать, внедрять, использовать, контролировать, проверять, поддерживать и совершенствовать СМИБ;
- b) обеспечить согласованность принципов информационной безопасности с требованиями бизнеса;
- c) определять юридические и регулятивные требования и договорные обязанности по безопасности;
- d) поддерживать необходимый уровень безопасности путем правильного применения всех внедрённых средств управления;
- e) по необходимости проводить проверки, и соответствующе реагировать на результаты этих проверок; и
- f) где необходимо, совершенствовать эффективность СМИБ.

#### **5.2.2 Обучение, информированность и компетентность**

Организация должна гарантировать то, что весь персонал, назначенный исполнять установленные в СМИБ обязанности, достаточно компетентен, чтобы выполнять поставленные задачи, путём:

- a) установления необходимого уровня компетентности персонала, выполняющего работу, влияющую на функционирование СМИБ;
- b) проведения обучения или принятия других мер (например, назначение компетентного персонала), чтобы удовлетворить эти нужды;
- c) оценивания эффективности предпринятых действий; и
- d) ведения записей о подготовке, обучении, навыках, опыте и квалификации (см. 4.3.3).

Организация также должна убедиться в том, что все компетентные работники осознают значимость и важность своей деятельности по обеспечению информационной безопасности, и их вклада в достижение целей СМИБ.

## **6 Внутренние аудиты СМИБ**

Организация должна проводить внутренние аудиты СМИБ для того, чтобы убедиться, что задачи, средства управления, процессы и методы СМИБ:

- a) удовлетворяют требованиям данного Международного Стандарта и важным законам или положениям;
- b) удовлетворяют установленным требованиям информационной безопасности;
- c) эффективно выполняются и поддерживаются; и
- d) функционируют, как ожидалось.

Программа аудита должна быть спланирована, учтены как состояние и важность процессов и областей, подвергаемых аудиту, так и результаты предыдущих аудитов. Должны быть определены критерии аудита, масштаб, частота проведения, методики. Выбор аудиторов и проведение аудитов должны гарантировать объективность и беспристрастность процесса аудита. Аудиторы не должны ревизовать свою собственную работу.

Порядок распределения обязанностей и требования к планированию и проведению аудитов, к отчетам о результатах и ведению записей (см. 4.3.3) должны быть определены в документально оформленной процедуре.

Руководство, ответственное за подвергаемую аудиту область, должно гарантировать, что без большой задержки предпримет действия по устранению выявленных несогласованностей и их причин. Последующие ревизии должны требовать подтверждения того, что действительно были предприняты соответствующие меры, и отчёты о полученных результатах (см. 8).

**ПРИМЕЧАНИЕ:** МОС 19011:2002, Рекомендации по ревизованию качества и/или систем менеджмента экологии, могут быть полезными в проведении внутренних аудитов СМИБ.

## **7 Проверка управления СМИБ**

### **7.1 Общие положения**

Руководство должно проверять СМИБ в запланированные периоды (как минимум раз в год), чтобы убедиться в том, что она по-прежнему пригодна, адекватна и эффективна. Такая проверка должна включать оценку возможностей совершенствования и необходимости изменений в СМИБ, в т.ч. и в политике информационной безопасности и целях информационной безопасности. Результаты проверки необходимо оформить документально, и сделать записи (см. 4.3.3).

### **7.2 Входные данные для проверки**

Входные данные для проверки управления должны включать:

- a) результаты аудитов и проверок СМИБ;
- b) рекомендации заинтересованных сторон;
- c) технику, продукты или методики, которые могли бы использоваться в организации, чтобы совершенствовать функционирование и эффективность СМИБ;
- d) состояние превентивных и корректирующих мер;
- e) уязвимости или угрозы, недостаточно исследованные при предыдущей оценке риска;
- f) результаты оценки эффективности;
- g) контроль принятия соответствующих мер после предыдущих проверок управления;
- h) любые изменения, которые могут повлиять на СМИБ; и
- i) рекомендации по совершенствованию.

### **7.3 Выходные данные проверки**

Итоги проверки управления должны включать любые решения и меры, связанные со следующим.

- a) Совершенствование эффективности СМИБ;
- b) Обновление планов оценки и сокращения риска;
- c) Модификация методов и средств управления, влияющих на информационную безопасность, как необходимость реагирования на внутренние и внешние события, которые могут принести ущерб СМИБ, а также изменения в:
  - 1) требованиях бизнеса;
  - 2) требованиях безопасности;
  - 3) бизнес-процессах, влияющих на существующие требования бизнеса;
  - 4) юридических или регулятивных требованиях;
  - 5) договорных обязательствах; и
  - 6) уровнях риска и/или критериях допустимости риска.
- d) Приобретение необходимых ресурсов.
- e) Совершенствование системы оценивания эффективности.

## **8 Совершенствование СМИБ**

### **8.1 Постоянное совершенствование**

Организация должна постоянно совершенствовать эффективность СМИБ, привлекая к этому процессу политику информационной безопасности, цели информационной безопасности, результаты аудита, анализ отслеженных событий, корректирующие и превентивные мероприятия и проверки управления (см. 7).

### **8.2 Корректирующие меры**

Организация должна предпринимать меры по устранению причин несоответствия требованиям СМИБ, чтобы избежать повторения. Документированная процедура проведения корректирующих мероприятий должна содержать требования по:

- a) выявлению несоответствий;
- b) определению причин несоответствий;
- c) оценке необходимости мер, устраняющих несоответствия;
- d) определению и проведению необходимых корректирующих мероприятий;
- e) записи результатов предпринятых мер (см. 4.3.3); и
- f) проверке предпринятых корректирующих мер.

### **8.3 Превентивные мероприятия**

Организация должна определить меры, направленные на устранение причин возможного несоответствия требованиям СМИБ, чтобы предотвратить их повторение. Превентивные действия должны соответствовать ущербу от возможных ударов. Документированная процедура проведения превентивных мероприятий должна содержать требования по:

## ISO/IEC 27001:2005(E)

- a) выявлению возможных несоответствий и их причин;
- b) оценке необходимости действий, предотвращающих повторение несоответствий;
- c) определению и проведению необходимых превентивных мероприятий;
- d) записи результатов предпринятых мер (4.3.3); и
- e) проверке предпринятых превентивных мер.

Организация должна выявить изменения в рисках и определить требования по превентивным действиям, акцентируя внимание на значительно измененных рисках.

Приоритеты превентивных мероприятий должны быть расставлены согласно результатам оценки риска.

**ПРИМЕЧАНИЕ:** Меры по предупреждению несоответствий часто более эффективны и дешевле обходятся, чем уже корректирующие мероприятия.

# Приложение А (нормативное)

## Задачи (цели) и средства управления

Цели и средства управления, перечисленные в таблице А.1, непосредственно выводятся и подгоняются под цели и средства, перечисленные в разделах с 5 по 15 стандарта МОС/МЭК 17799:2005. Список из таблицы А.1 не является исчерпывающим, потому что организация может предусмотреть дополнительные цели и средства управления. А перечисленные в данных таблицах необходимо выбрать как составляющий компонент СМИБ, определённой в 4.2.1.

Разделы МОС/МЭК 17799:2005 с 5 по 15 предусматривают руководство по внедрению и наилучшему использованию средств управления, определённых с пункта А.5 по пункт А.15.

Таблица А.1 – Цели и средства управления

<b>А.5 Политика безопасности</b>		
<b>А.5.1 Политика информационной безопасности</b>		
<i>Цель:</i> Обеспечить управление и поддержку руководством информационной безопасности в соответствии с бизнес-требованиями и важными законами и положениями.		
A.5.1.1	Документ политики информационной безопасности	<i>Средство управления</i> Политика информационной безопасности должна быть одобрена руководством, издана и передана все сотрудникам и важным сторонним организациям.
A.5.1.2	Пересмотр политики информационной безопасности	<i>Средство управления</i> Необходимо проводить пересмотр политики безопасности в запланированные периоды либо в случае серьёзных изменений, чтобы убедиться в её пригодности, адекватности и эффективности.
<b>А.6 Организация информационной безопасности</b>		
<b>А.6.1 Внутренняя организация</b>		
<i>Цель:</i> управление информационной безопасностью в пределах организации.		
A.6.1.1	Обязанности руководства по обеспечению информационной безопасности	<i>Средство управления</i> Руководство должно активно поддерживать безопасность в пределах организации посредством чёткого управления, выполнения обязательств, явного распределения и уведомления об обязанностях по обеспечению безопасности.
A.6.1.2	Согласованность мероприятий по защите информации	<i>Средство управления</i> Мероприятия по защите информации должны быть согласованы представителями различных отделов организации, занимающих наиболее ответственные должности.
A.6.1.3	Распределение обязанностей по защите информации	<i>Средство управления</i> Все обязанности по обеспечению защиты информации должны быть чётко распределены.
A.6.1.4	Процесс утверждения средств обработки информации	<i>Средства управления</i> Необходимо определить и задействовать процесс управления одобрением и утверждением новых средств обработки информации.
A.6.1.5	Соглашения по конфиденциальности	<i>Средства управления</i> Необходимо определить и постоянно пересматривать требования конфиденциальности или сокрытия соглашений, отражающих нужды организации в защите информации.
A.6.1.6	Связь с ведомствами	<i>Средства управления</i> Необходимо поддерживать соответствующие контакты с важными ведомствами.
A.6.1.7	Связь с особо заинтересованными	<i>Средства управления</i> Необходимо поддерживать соответствующие контакты с особо

	группами	заинтересованными сторонами или другими форумами безопасности и профессиональными объединениями.
A. 6.1.8	Независимая проверка информационной безопасности	<b>Средства управления</b> В запланированные периоды или в результате серьёзных изменений в безопасности, необходимо проводить независимую проверку методики управления информационной безопасностью в организации и её внедрения (напр., задачи управления, средства управления, политики, методологии и приёмы защиты информации).
<b>A.6.2 Сторонние организации</b> <i>Цель:</i> Поддерживать безопасность информации и средств обработки информации, которые доступны, обрабатываются, передаются или управляются сторонними организациями.		
A.6.2.1	Определение рисков, связанных с привлечением сторонних организаций	<b>Средства управления</b> Необходимо выявить риски безопасности информации и средств обработки информации, разработанных с привлечением сторонних организаций, а также определить соответствующие средства управления и внедрить их раньше, чем будет предоставлен доступ.
A. 6.2.2	Обеспечение безопасности во время работы с заказчиками	<b>Средства управления</b> Необходимо обеспечить выполнение всех установленных требований безопасности раньше, чем заказчикам будет предоставлен доступ к информации или активам организации.
A. 6.2.3	Обеспечение безопасности при подписании соглашений со сторонними организациями	<b>Средства управления</b> Соглашения с третьими лицами, затрагивающие доступ, обработку, передачу или управление информацией либо средствами обработки информации или же приложение других продуктов либо служб к средствам обработки информации должны покрывать все наиболее важные требования безопасности.
<b>A.7 Asset management</b>		
<b>A.7.1 Ответственность за активы</b> <i>Цель:</i> Достичь и поддерживать соответствующий уровень защиты активов организации.		
A.7.1.1	Опись активов	<b>Средство управления</b> Необходимо чётко идентифицировать все активы, провести инвентаризацию.
A.7.1.2	Владение активами	<b>Средство управления</b> Вся информация и активы, связанные со средствами обработки информации должны 'числиться' <sup>3)</sup> за а назначенным отделом организации.
A.7.1.3	Допустимое использование активов	<b>Средство управления</b> Необходимо разработать, документально оформить и ввести правила использования информации и активов, связанных со средствами обработки информации.
<b>A.7.2 Классификация информации</b> <i>Цель:</i> Обеспечить соответствующий уровень защищённости информации.		
A.7.2.1	Руководства по классификации	<b>Средство управления</b> Необходимо классифицировать информацию в зависимости от её ценности, юридических требований, критичности и необходимости для организации.
A.7.2.2	Маркирование и обработка информации	<b>Средство управления</b> Необходимо классифицировать информацию в зависимости от её ценности, юридических требований, критичности и необходимости для организации.
<b>A.8 Защита трудовых ресурсов</b>		

**А.8.1 До наёма на работу<sup>4)</sup>**

*Цель:* Обеспечить понимание сотрудниками, подрядными и сторонними организациями своих обязательств, определить их пригодность к выполнению предполагаемой работы, сократить риск кражи, подделки, или неправильного обращения с аппаратурой.

А.8.1.1	Роли и обязанности	<p><i>Средство управления</i> В соответствии с политикой информационной безопасности организации должны быть определены и документально оформлены роли и обязательства сотрудников, а также подрядных и сторонних организаций.</p>
---------	--------------------	--

3) Объяснение: Термин «владелец» отождествляется с индивидом или субъектом, которая утверждена нести ответственность за контроль производства, развития, технического обслуживания, применения и безопасности активов. Термин «владелец» не означает, что персона действительно имеет какие-либо права собственности на актив.

4) Объяснение: Термин 'наём' употреблён в смысле: приём на работу сотрудников (на временной или постоянной основе), назначение на должность, перевод на другую должность, приём на работу по договору подряда, а также истечение срока действия этих договорённостей.

А.8.1.2	Фильтрация	<p><i>Средство управления</i> Проверка личных данных всех кандидатов на работу в штате, по договору подряда либо в качестве сторонней организации должна проводиться в соответствии с соответствующими законами, положениями и нормами этики, пропорционально бизнес-требованиям, уровню доступа и осознаваемым рискам.</p>
А.8.1.3	Сроки и условия приёма на работу	<p><i>Средство управления</i> Неотъемлемая часть договорного обязательства – принятие условий приёма на работу, и подписание трудового контракта, устанавливающего обязанности сотрудников, работающих в штате, по договору подряда либо в сторонних организациях, а также самой организации по обеспечению информационной безопасности.</p>

**А.8.2 Непосредственная работа в организации**

*Цель:* Обеспечить осведомлённость всех штатных сотрудников, подрядных и сторонних организаций об угрозах и уязвимостях безопасности информации, их обязанностях и обязательствах; достаточность знаний для поддержки безопасности и сокращения риска ошибки человека.

А.8.2.1	Обязанности руководства	<p><i>Средство управления</i> Руководство должно требовать от штатных сотрудников, подрядных и сторонних организаций осуществления функций защиты в соответствии с политиками и положениями, определёнными в организации.</p>
А.8.2.2	Знание, образованность и обучение	<p><i>Средство управления</i> Все штатные сотрудники организации, а в некоторых случаях и подрядные и сторонние организации должны постоянно повышать свою квалификацию, укреплять знания, иметь возможность своевременно ознакомиться с изменениями в политиках, методах, имеющих непосредственное отношение к их работе.</p>
А.8.2.3	Дисциплинарные процедуры	<p><i>Средство управления</i> Необходимо предусмотреть строгую дисциплинарную процедуру за нарушение сотрудником безопасности.</p>

**А.8.3 Истечение срока либо переход на другую должность**

*Цель:* Обеспечить соблюдение определённого порядка при увольнении и переводе на другую должность штатных сотрудников, подрядных и сторонних организаций.

А.8.3.1	Обязанности при окончании срока работы по найму	<p><i>Средство управления</i> Должны быть чётко прописаны обязанности сотрудников при окончании срока работы либо при переводе на другую должность.</p>
А.8.3.2	Возврат активов	<p><i>Средство управления</i> После окончания срока действия трудового контракта либо соглашения все штатные сотрудники организации, подрядные и сторонние организации обязаны вернуть все активы</p>

		организации, находившиеся в их распоряжении.
A.8.3.3	Лишение прав доступа	<i>Средство управления</i> После окончания срока действия трудового контракта или соглашения права доступа всех штатных сотрудников, подрядных и сторонних организаций к информации и средствам обработки информации должны быть ликвидированы либо настроены в соответствии с новой должностью.
<b>A.9 Защита от несанкционированного физического доступа и природных катастроф</b>		
<b>A.9.1 Зоны безопасности</b>		
<i>Цель:</i> Предотвратить несанкционированный физический доступ, повреждение и проникновение в помещение организации, вмешательство в работу с информацией.		
A.9.1.1	Периметр физической безопасности	<i>Средство управления</i> Для защиты участков хранения информации и средств её обработки необходимо использовать периметры безопасности (барьеры, такие как стены, таблетки, вахта).
A.9.1.2	Контроль проникновения в помещение	<i>Средство управления</i> Для защиты зон безопасности необходимо контролировать доступ в помещение, обеспечив свободный вход лишь уполномоченным сотрудникам.
A.9.1.3	Организация защиты офисов, кабинетов и оборудования	<i>Средство управления</i> Необходимо разработать и применить план физической защиты офисов, кабинетов, оборудования.
A.9.1.4	Защита от внешних угроз и угроз окружающей среды	<i>Средство управления</i> Необходимо разработать и применить план физической защиты от пожара, потопа, землетрясения, взрыва, беспорядков среди граждан и других форм природных и искусственных катастроф.
A.9.1.5	Работа в безопасной зоне	<i>Средство управления</i> Необходимо разработать и применить план и принципы физической защиты при работе в зонах безопасности.
A.9.1.6	Зоны общего доступа, доставки и погрузки	<i>Средство управления</i> В точках доступа, таких как зона доставки и погрузки и других, куда могут проникнуть посторонние лица, необходимо контролировать помещение, а по возможности и очистить его от средств обработки информации, чтобы предотвратить несанкционированный доступ.
<b>A.9.2 Безопасность оборудования</b>		
<i>Цель:</i> Предотвратить потерю, повреждение, воровство или рассекречивание активов и задержки в работе организации.		
A.9.2.1	Размещение оборудования и его защита	<i>Средство управления</i> Необходимо так размещать оборудование и организовывать его защиту, чтобы сократить последствия стихийных бедствий, а также предотвратить возможность несанкционированного доступа.
A.9.2.2	Вспомогательные службы	<i>Средство управления</i> Оборудование необходимо защищать от сильных повреждений и поломок, обусловленных сбоями в работе коммунальных служб.
A.9.2.3	Безопасность кабельных сетей	<i>Средство управления</i> Важные данные, передаваемые по линиям связи или информационные службы поддержки, должны быть защищены от перехвата или повреждения.
A.9.2.4	Тех. обслуживание оборудования	<i>Средство управления</i> Для обеспечения пригодности и целостности оборудования необходимо правильно его эксплуатировать.
A.9.2.5	Безопасность выносного оборудования	<i>Средство управления</i> Необходимо обеспечить защиту выносного оборудования с учётом различных рисков его эксплуатации вне помещения организации.
A.9.2.6	Передача оборудования или использование б/у оборудования	<i>Средство управления</i> Необходимо проверять все комплектующие оборудования, содержащие средства хранения информации, чтобы убедиться в том, что засекреченные данные и лицензионное программное

		обеспечение были удалены либо безопасным образом переписаны до ликвидации/передачи оборудования.
A.9.2.7	Ликвидация оборудования	<i>Средство управления</i> Оборудование, информация или ПО не должно уничтожаться без разрешения руководства.
<b>A.10 Менеджмент обмена и оперирования информацией</b>		
<b>A.10.1 Положения об эксплуатации и обязанности</b>		
<i>Цель:</i> Обеспечить корректное и безопасное использование средств обработки информации.		
A.10.1.1	Документальное оформление техники эксплуатации	<i>Средство управления</i> Техника эксплуатация должна быть документально оформлена, храниться и быть доступна всем нуждающимся в ней пользователям.
A.10.1.2	Менеджмент изменений	<i>Средство управления</i> Необходимо контролировать модификации в средствах обработки информации и системах.
A.10.1.3	Разделение обязанностей	<i>Средство управления</i> Должны быть разделены обязанности и сферы ответственности, чтобы сократить вероятность несанкционированной или непреднамеренной модификации или некорректного использования активов организации.
A.10.1.4	Разделение разрабатываемых, тестируемых и рабочих средств	<i>Средство управления</i> Необходимо разделять разрабатываемые, тестируемые и рабочие средства, чтобы сократить риски несанкционированного доступа или модификации в рабочей системе.
<b>A.10.2 Менеджмент поставки услуг третьими лицами</b>		
<i>Цель:</i> Установить и поддерживать соответствующий уровень информационной безопасности и поставки услуг при заключении договоров об оказании услуг поставки с третьими лицами.		
A.10.2.1	Поставка услуг	<i>Средство управления</i> Необходимо обеспечить достижение, осуществление и поддержку третьими лицами включённых в договор об оказании услуг уровней безопасности средств управления, описания задания и поставки.
A.10.2.2	Мониторинг и проверка работы третьих лиц	<i>Средство управления</i> Работы, отчёты и записи, выполняемые третьими лицами должны постоянно контролироваться и проверяться, необходимо регулярно проводить аудиты.
A.10.2.3	Управление изменениями в работе третьих лиц	<i>Средство управления</i> Изменениями в условиях работы, включая поддержку и совершенствование существующих политик информационной безопасности, методах и средствах управления, необходимо управлять с учётом критичности вовлечённых в работу бизнес-систем и процессов, а также оценок рисков.
<b>A.10.3 Планирование и приёмка системы</b>		
<i>Цель:</i> Минимизировать риск отказа систем.		
A.10.3.1	Менеджмент способностей	<i>Средство управления</i> Необходимо контролировать и регулировать использование ресурсов, оценивать требования будущих способностей, чтобы обеспечить требуемые характеристики системы.
A.10.3.2	Приёмка системы	<i>Средство управления</i> Должны быть установлены критерии приёмки новых информационных систем, обновлённых и новых версий, произведены необходимые испытания системы во время её разработки и до прёмки.
<b>A.10.4 Защита от умышленных ошибок и лёгкости изменения в коде</b>		
<i>Цель:</i> Защитить целостность ПО и информации.		
A.10.4.1	Меры против совершения умышленных ошибок в коде программы	<i>Средство управления</i> Необходимо внедрить средства обнаружения, предотвращения и восстановления, чтобы обезопасить код от умышленных ошибок и знания пользователем соответствующих процедур.
A.10.4.2	Меры против лёгкости изменения кода	<i>Средство управления</i> В случае разрешения использования простого кода необходимо

	программы	убедиться в том, что разрешённый простой код выполняется в соответствии с чётко определённой политикой безопасности, в противном случае необходимо предотвратить выполнение простого кода.
<b>A.10.5 Дублирование</b> <i>Цель:</i> Поддерживать целостность и доступность информации и средств обработки информации.		
A.10.5.1	Дублирование информации	<i>Средство управления</i> В соответствии с политикой резервного копирования необходимо регулярно делать и тестировать резервные копии информации и ПО.
<b>A.10.6 Менеджмент безопасности сети</b> <i>Цель:</i> Обеспечить защиту информации в сетях и защиту поддерживающей инфраструктуры.		
A.10.6.1	Средства управления работы сети	<i>Средство управления</i> Необходимо соответствующим образом контролировать и управлять работой сети, чтобы обеспечить защиту от угроз, и поддерживать безопасность систем и приложений, использующих сеть, а также безопасность передающейся информации.
A.10.6.2	Безопасность сетевых служб	<i>Средство управления</i> Необходимо определить особенности защиты, уровни безопасности и требования менеджмента для всех сетевых служб, а также включать их в любые договоры оказания услуг связи, независимо от того, обеспечена работа этих служб силами организации либо внешними источниками.
<b>A.10.7 Обращение с носителями информации</b> <i>Цель:</i> Предотвратить несанкционированное раскрытие, изменение, удаление или разрушение активов, предотвратить задержки в работе организации.		
A.10.7.1	Менеджмент съёмных носителей информации	<i>Средство управления</i> Необходимо предусмотреть процедуры работы с данными на съёмных носителях.
A.10.7.2	Уничтожение носителей информации	<i>Средство управления</i> Необходимо предусмотреть строгие процедуры проведения безопасного уничтожения данных, когда отпадает в них необходимость.
A.10.7.3	Процедуры обработки информации	<i>Средство управления</i> Чтобы защитить информацию от несанкционированного раскрытия или некорректного использования необходимо предусмотреть процедуры работы с данными и их хранения.
A.10.7.4	Безопасность системной документации	<i>Средство управления</i> Необходимо обезопасить системную документацию от несанкционированного доступа.
<b>A.10.8 Обмен информацией</b> <i>Цель:</i> Обеспечить безопасность информации и ПО при обмене ими в пределах организации или со сторонними организациями.		
A.10.8.1	Политики и процедуры обмена информацией	<i>Средство управления</i> Необходимо предусмотреть политики, строгие процедуры и средства управления обменом информацией, чтобы защитить данные при использовании различных средств связи.
A.10.8.2	Соглашения по обмену Exchange agreements	<i>Средство управления</i> Необходимо заключить договоры по обмену информацией и ПО между организацией и внешними организациями.
A.10.8.3	Передаваемые физические носители информации Physical media in transit	<i>Средство управления</i> Необходимо защищать носители информации от несанкционированного доступа, некорректного использования или порчи во время перевозки вне стен организации.
A.10.8.4	Электронный обмен сообщениями	<i>Средство управления</i> Необходимо соответствующим образом защищать передаваемую в электронных сообщениях информацию.
A.10.8.5	Информационные бизнес-системы	<i>Средство управления</i> Необходимо разработать и привести в действие политики и процедуры для обеспечения защиты информации, использующейся при взаимодействии информационных

		бизнес-систем.
<b>А.10.9 Электронные коммерческие услуги</b>		
<i>Цель:</i> Обеспечить безопасность электронных коммерческих служб и их безопасного использования.		
А.10.9.1	Электронная коммерция	<i>Средство управления</i> Необходимо защищать связанную с электронной коммерцией информацию, проходящую через сеть общего пользования, от мошенничества, споров по контракту и несанкционированного раскрытия и модификации.
А.10.9.2	Оперативные транзакции	<i>Средство управления</i> Необходимо защищать передающуюся в режиме онлайн информацию, чтобы предотвратить незавершенную передачу, неправильное направление, несанкционированное изменение сообщений, раскрытие, копирование или воспроизведение информации.
А.10.9.3	Общественно-доступная информация	<i>Средство управления</i> Необходимо защищать от несанкционированной модификации информацию, доступную для общего использования.
<b>А.10.10 Мониторинг</b>		
<i>Цель:</i> Обнаружить несанкционированные попытки обработки информации.		
А.10.10.1	Ведение контрольных журналов	<i>Средство управления</i> Необходимо вести и хранить до установленного срока контрольные журналы, регистрирующие действия пользователей, исключительные события и инциденты в информационной безопасности, помогающие в будущем при расследованиях и мониторинге доступа.
А.10.10.2	Мониторинг использования системы	<i>Средство управления</i> Необходимо разработать процедуры мониторинга использования средств обработки информации, регулярно просматривать результаты мониторинга действий.
А.10.10.3	Защита журналов регистрации	<i>Средство управления</i> Средства регистрации и журналы регистрации должны быть защищены от несанкционированного доступа и использования.
А.10.10.4	Регистрация действий администраторов и операторов	<i>Средство управления</i> Необходимо регистрировать все действия системного администратора и системных операторов.
А.10.10.5	Регистрация ошибок	<i>Средство управления</i> Необходимо регистрировать и анализировать ошибки, предпринимать соответствующие меры.
А.10.10.6	Синхронизация времени	<i>Средство управления</i> По установленному источнику точного времени необходимо синхронизировать время всех систем обработки информации в пределах организации либо области безопасности.
<b>А.11 Управление доступом</b>		
<b>А.11.1 Бизнес-требования управления доступом</b>		
<i>Цель:</i> Осуществлять управление доступом к информации.		
А.11.1.1	Политика управления доступом	<i>Средство управления</i> Политика управления доступом должна быть разработана, документирована, и должна пересматриваться исходя из бизнес-требований и требований безопасности для доступа.
<b>А.11.2 Управление доступом пользователей</b>		
<i>Цель:</i> Обеспечить доступ авторизованных пользователей и предотвратить неавторизованный доступ к информационным системам.		
А.11.2.1	Регистрация пользователей	<i>Средство управления</i> Должна иметь место формальная процедура регистрации и отмены регистрации пользователей для предоставления и отмены доступа ко всем информационным системам и сервисам.
А.11.2.2	Управление привилегиями	<i>Средство управления</i> Необходимо ограничивать и контролировать распределение и использование привилегий.
А.11.2.3	Управление паролями пользователей	<i>Средство управления</i> Необходимо предусмотреть строгую процедуру управления

		назначением паролей.
A.11.2.4	Пересмотр прав доступа пользователей	<i>Средство управления</i> Руководство должно регулярно пересматривать права доступа пользователей, следуя формальной процедуре.
<b>A.11.3 Обязанности пользователей</b>		
<i>Цель:</i> Предотвратить доступ неавторизованных пользователей, а также компрометацию или хищение информации и средств обработки информации.		
A.11.3.1	Использование паролей	<i>Средство управления</i> При выборе и использовании паролей пользователи обязаны следовать инструкциям по безопасности.
A.11.3.2	Пользовательское оборудование, оставленное без присмотра	<i>Средство управления</i> Пользователи должны обеспечить соответствующую защиту оборудованию, оставленному без присмотра.
A.11.3.3	Политика чистого экрана и рабочего места	<i>Средство управления</i> Должна быть принята политика чистого рабочего места для бумаг и съемных носителей и политика чистого экрана для средств обработки информации.
<b>A.11.4 Управление доступом по сети</b>		
<i>Цель:</i> Предотвратить неавторизованный доступ к сетевым сервисам.		
A.11.4.1	Политика использования сетевых сервисов	<i>Средство управления</i> Пользователям должен предоставляться доступ только к тем сервисам, которые им разрешено использовать.
A.11.4.2	Идентификация пользователей для внешних соединений	<i>Средство управления</i> Для управления доступом удаленных пользователей должны использоваться соответствующие методы аутентификации.
A.11.4.3	Идентификация оборудования в сетях	<i>Средство управления</i> Автоматическая идентификация оборудования должна рассматриваться как средство аутентификации соединений из определенных мест и оборудования.
A.11.4.4	Защита удаленных диагностических и конфигурационных портов	<i>Средство управления</i> Необходимо управлять физическим и логическим доступом к диагностическим и конфигурационным портам.
A.11.4.5	Сегрегация в сетях	<i>Средство управления</i> Группы информационных сервисов, пользователей и информационные системы должны быть сегрегированы в сетях.
A.11.4.6	Управление сетевыми соединениями	<i>Средство управления</i> Для общих сетей, особенно тех, которые выходят за границы организации, должны быть ограничены возможности подсоединения пользователей к сети, наряду с политикой контроля доступа и требованиями бизнес-приложений (см. 11.1).
A.11.4.7	Управление сетевой маршрутизацией	<i>Средство управления</i> Необходимо внедрять средства управления маршрутизацией в сетях, чтобы обеспечить, что компьютерные соединения и информационные потоки не противоречат политике управления доступом бизнес-приложений.
<b>A.11.5 Управление доступом к операционным системам</b>		
<i>Цель:</i> Предотвратить неавторизованный доступ к операционным системам.		
A.11.5.1	Процедуры защищенного входа в систему	<i>Средство управления</i> Управление доступом к операционным системам должно осуществляться с помощью процедуры защищенного входа в систему.
A.11.5.2	Идентификация и аутентификация пользователей	<i>Средство управления</i> Все пользователи должны иметь уникальный идентификатор (ID пользователя) только для их личного пользования, а также должна быть выбрана подходящая техника аутентификации для подтверждения заявленной личности пользователя.
A.11.5.3	Система управления паролями	<i>Средство управления</i> Системы управления паролями должны быть интерактивны и должны обеспечивать качество паролей.

A.11.5.4	Использование системных утилит	<i>Средство управления</i> Использование утилит, которые могут быть допущены к важнейшим средствам управления системой и приложениями, должно быть ограничено и полностью контролироваться.
A.11.5.5	Блокировка сессий по времени	<i>Средство управления</i> Неактивные сессии должны завершаться по прошествии определенного времени бездействия.
A.11.5.6	Ограничение времени соединения	<i>Средство управления</i> Необходимо использовать ограничения на время соединения для обеспечения дополнительной защиты для приложений с высоким уровнем риска.
<b>A.11.6 Управление доступом к приложениям и информации</b> <i>Цель:</i> Предотвратить неавторизованный доступ к информации, содержащейся в системах приложений.		
A.11.6.1	Ограничение доступа к информации	<i>Средство управления</i> Доступ пользователей и обслуживающего персонала к информации и функциям системы приложений должен быть ограничен shall be restricted в соответствии с определенной политикой управления доступом.
A.11.6.2	Изоляция чувствительных участков системы	<i>Средство управления</i> Чувствительные участки систем должны иметь выделенную (изолированную) вычислительную среду.
<b>A.11.7 Мобильная вычислительная техника и телефония</b> <i>Цель:</i> Обеспечить защиту информации во время использования средств мобильной вычислительной техники и телефонии.		
A.11.7.1	Мобильная вычислительная техника и коммуникации	<i>Средство управления</i> Необходимо предусмотреть строгую политику безопасности, а также принять соответствующие мероприятия по безопасности для защиты от рисков, связанных с использованием средств мобильной вычислительной техники и коммуникации.
A.11.7.2	Работа по телефону	<i>Средство управления</i> Должны быть разработаны и внедрены политика, операционные планы и процедуры для работы по телефону.
<b>A.12 Приобретение, расширение и эксплуатация информационных систем</b>		
<b>A.12.1 Требования безопасности информационных систем</b> <i>Цель:</i> обеспечить, чтобы безопасность являлась важной составляющей частью информационных систем.		
A.12.1.1	Спецификация и анализ требований безопасности	<i>Средство управления</i> Положения бизнес-требований для новых информационных систем или усовершенствований существующих информационных систем должны устанавливать требования для средств управления безопасностью.
<b>A.12.2 Правильная обработка данных в приложении</b> <i>Цель:</i> Предотвратить ошибки, потери, неавторизованное изменение или неправильное использование информации в приложениях.		
A.12.2.1	Проверка правильности входных данных	<i>Средство управления</i> Необходимо производить проверку достоверности входных данных приложений, чтобы гарантировать правильность и соответствие данных.
A.12.2.2	Контроль внутренней обработки данных	<i>Средство управления</i> Проверки правильности должны быть встроены в приложения для обнаружения какого-либо искажения информации из-за ошибок обработки или преднамеренных действий.
A.12.2.3	Целостность сообщений	<i>Средство управления</i> Необходимо идентифицировать требования для обеспечения достоверности и защиты целостности сообщений в приложениях, а также идентифицировать и внедрить соответствующие средства управления.
A.12.2.4	Проверка правильности выходных данных	<i>Средство управления</i> Необходимо производить проверку достоверности входных данных приложений, чтобы гарантировать, что обработка хранимой информации является правильной и соответствующей обстоятельствам.

<b>A.12.3 Средства криптографии</b>		
<i>Цель:</i> Защитить конфиденциальность, подлинность или целостность информации с помощью криптографических средств.		
A.12.3.1	Политика использования средств криптографии	<i>Средство управления</i> Для защиты информации необходимо разработать и внедрить политику использования средств криптографии.
A.12.3.2	Управление ключами	<i>Средство управления</i> Необходимо наличие управления ключами для поддержки используемых в организации криптографических технологий.
<b>A.12.4 Защита системных файлов</b>		
<i>Цель:</i> Обеспечить защиту системных файлов.		
A.12.4.1	Управление программным обеспечением	<i>Средство управления</i> Должны иметься процедуры для управления установкой программного обеспечения в операционных системах.
A.12.4.2	Защита тестовых данных системы	<i>Средство управления</i> Тестовые данные должны быть выбраны тщательным образом, а также защищены и проверены.
A.12.4.3	Управление доступом к исходным кодам программ	<i>Средство управления</i> Необходимо ограничить доступ к исходным кодам программ.
<b>A.12.5 Безопасность процессов разработки и поддержки</b>		
<i>Цель:</i> Поддерживать безопасность программного обеспечения прикладных систем и информации.		
A.12.5.1	Процедуры контроля изменений	<i>Средство управления</i> Необходимо контролировать внесение изменений, используя формальные процедуры контроля изменений.
A.12.5.2	Специальный осмотр программных приложений после изменений в операционной системе	<i>Средство управления</i> После внесения изменений в операционные системы необходимо пересмотреть и протестировать критичные для бизнеса приложения, чтобы убедиться, что не было оказано неблагоприятного воздействия на деятельность или безопасность организации.
A.12.5.3	Ограничения на изменения пакетов программного обеспечения	<i>Средство управления</i> Изменения пакетов программного обеспечения нужно избегать, ограничиться самыми необходимыми изменениями, а также все изменения должны строго контролироваться.
A.12.5.4	Утечка информации	<i>Средство управления</i> Необходимо предотвратить возможности для утечки информации.
A.12.5.5	Аутсорсинговая разработка программного обеспечения	<i>Средство управления</i> Организация должна заведовать и следить за аутсорсинговой разработкой программного обеспечения.
<b>A.12.6 Управление техническими уязвимостями</b>		
<i>Цель:</i> Снизить риски, возникающие в результате использования опубликованных технических уязвимостей.		
A.12.6.1	Контроль технических уязвимостей	<i>Средство управления</i> Необходимо получать своевременную информацию о технических уязвимостях используемых информационных систем, оценить подверженность организации воздействию данных угроз, а также принять соответствующие меры по сокращению связанных с ними рисков.
<b>A.13 Менеджмент инцидентов информационной безопасности</b>		
<b>A.13.1 Оповещение о событиях и уязвимостях информационной безопасности</b>		
<i>Цель:</i> Обеспечить своевременное оповещение о событиях и уязвимостях информационной безопасности для принятия соответствующих корректирующих мер.		
A.13.1.1	Оповещение о событиях информационной безопасности	<i>Средство управления</i> Необходимо максимально быстро по соответствующим каналам передавать руководству информацию о событиях в информационной безопасности.
A.13.1.2	Оповещение об уязвимостях защиты	<i>Средство управления</i> Необходимо требовать от всех штатных сотрудников, подрядных и сторонних организаций, работающих с информационными системами и службами, отслеживания и

		уведомления о наблюдаемой или подозрительной неустойчивости безопасности в информационных системах, службах.
<b>A.13.2 Менеджмент инцидентов информационной безопасности и совершенствований</b>		
<i>Цель:</i> Обеспечить использование непротиворечивой и эффективной методики менеджмента инцидентов информационной безопасности.		
A.13.2.1	Обязанности и механизмы работы	<i>Средство управления</i> Должны быть определены обязанности и механизмы работы руководства, чтобы обеспечить быструю, эффективную и спокойную реакцию на инциденты информационной безопасности.
A.13.2.2	Изучение инцидентов информационной безопасности	<i>Средство управления</i> Должны быть предусмотрены механизмы оценки и мониторинга типов, масштабов и ущерба от инцидентов информационной безопасности.
A.13.2.3	Сбор улик	<i>Средство управления</i> В случаях, когда наказание индивида либо организации за случившийся инцидент безопасности требует правового вмешательства (либо привлечения к административной или уголовной ответственности), необходимо произвести сбор улик, сохранение их и представление их в соответствии с правилами сбора доказательств, установленными в соответствующих органах правосудия.
<b>A.14 Управление непрерывностью бизнеса (бесперебойной работой организации)</b>		
<b>A.14.1 Аспекты информационной безопасности при обеспечении непрерывности бизнеса</b>		
<i>Цель:</i> Нейтрализовать заминки при осуществлении бизнес-операций, защитить критичные бизнес-процессы от последствий крупных повреждений или аварий в информационных системах, обеспечить их своевременное восстановление.		
A.14.1.1	Включение информационной безопасности в процесс управления непрерывностью бизнеса	<i>Средство управления</i> Необходимо начать и поддерживать управляемый процесс обеспечения непрерывности бизнеса во всей организации, удовлетворяющий требованиям информационной безопасности, необходимым для обеспечения бесперебойной работы организации.
A.14.1.2	Непрерывность бизнеса и оценка рисков	<i>Средство управления</i> Необходимо выявлять события, способные вызвать заминки в деловой деятельности организации, вероятность и ущерб таких промедлений, и их влияние на информационную безопасность.
A.14.1.3	Разработка и осуществление планов непрерывности бизнеса, включающих и обеспечение безопасности	<i>Средство управления</i> Необходимо разрабатывать и обеспечивать выполнение планов поддержки и восстановления операций, обеспечивать требуемый уровень доступности информации после перебоев в работе или повреждений, критичных для осуществления деловых операций.
A.14.1.4	Схема планирования непрерывности бизнеса	<i>Средство управления</i> Должна поддерживаться единая схема планирования непрерывности бизнеса, способная обеспечить непротиворечивость планов, последовательную обработку требований информационной безопасности, правильного определения первостепенных задач тестирования и поддержки.
A.14.1.5	Тестирование, поддержка и пересмотр планов непрерывности	<i>Средство управления</i> Необходимо регулярно тестировать и обновлять планы непрерывности бизнеса, чтобы быть уверенными в их актуальности и эффективности.
<b>A.15 Соответствие</b>		
<b>A.15.1 Соответствие правовым требованиям</b>		
<i>Objective:</i> Избежать нарушения каких-либо законов, предписаний, регулятивных или договорных обязательств, а также каких-либо требований безопасности.		
A.15.1.1	Идентификация соответствующего законодательства	<i>Средство управления</i> Все соответствующие предписания, регулятивные и договорные требования и подход организации к удовлетворению этих требований должны быть подробно определены,

		документированы и поддерживаться актуальными для каждой информационной системы и организации.
A.15.1.2	Права интеллектуальной собственности (ПИС)	<i>Средство управления</i> Необходимо выполнять соответствующие процедуры, гарантирующие соответствие законодательству, регулятивным и договорным требованиям при использовании материалов, на которые могут иметься права интеллектуальной собственности, а также при использовании запатентованного программного обеспечения.
A.15.1.3	Защита документов организации	<i>Средство управления</i> Важные документы должны быть защищены от утери, уничтожения и фальсификации, в соответствии с предписаниями, регулятивными, договорными, и бизнес-требованиями.
A.15.1.4	Защита данных и конфиденциальность личной информации	<i>Средство управления</i> Защита данных и конфиденциальность должны обеспечиваться в соответствии с требованиями соответствующего законодательства, инструкций, а также договорных статей.
A.15.1.5	Предотвращение злоупотребления средствами обработки информации processing facilities	<i>Средство управления</i> Пользователи должны быть отстранены от использования средств обработки информации не по назначению.
A.15.1.6	Инструкции по применению средств криптографии	<i>Средство управления</i> Средства криптографии должны использоваться в соответствии со всеми соответствующими соглашениями, законами и инструкциями.
<b>A.15.2 Соответствие политике безопасности и стандартам, техническое соответствие</b> <i>Цель:</i> Обеспечить соответствие систем политике безопасности организации и стандартам.		
A.15.2.1	Соответствие политике безопасности и стандартам	<i>Средство управления</i> Для достижения соответствия политике безопасности и стандартам руководство должно гарантировать, что все процедуры безопасности на участке, за который оно ответственно, выполняются правильно.
A.15.2.2	Проверка технического соответствия	<i>Средство управления</i> Необходимо регулярно проверять информационные системы на соответствие стандартам по внедрению безопасности.
<b>A.15.3 Предположения аудита информационных систем</b> <i>Цель:</i> Максимизировать эффективность и минимизировать взаимное влияние между процессом аудита и информационными системами.		
A.15.3.1	Средства управления аудитом информационных систем	<i>Средство управления</i> Требования и аудиторская деятельность, включающая проверку операционных систем, должны быть тщательно спланированы и согласованы, чтобы минимизировать риск нарушения бизнес-процессов.
A.15.3.2	Защита инструментов проведения аудита информационных систем	<i>Средство управления</i> Доступ к инструментам аудита информационных систем должен быть защищен во избежание любого злоупотребления или компрометации.

## Приложение В (информативное)

### Принципы OECD и данного Международного Стандарта

Выдвинутые в Руководстве OECD принципы по обеспечению защиты информационных систем и сетей применимы ко всем политикам и действующим уровням управления защитой информационных систем и сетей. Данный Международный Стандарт обеспечивает структуру системы менеджмента информационной безопасности для внедрения некоторых принципов OECD с использованием модели PDCA и методик, описанных в разделах 4, 5, 6 и 8, как описано в таблице В.1.

**Таблица В.1 — принципы OECD и модель PDCA**

Принципы OECD	Соответствие функций СМИБ этапам PDCA
<p><b>Информированность</b></p> <p>Участники должны быть ознакомлены с нуждами безопасности информационных систем и сетей и знать, что они могут сделать для повышения безопасности.</p>	<p>Эта функция выполняется на этапе “Делай” (см. 4.2.2 и 5.2.2).</p>
<p><b>Обязанности</b></p> <p>Все участники ответственны за безопасность информационных систем и сетей.</p>	<p>Эта функция выполняется на этапе “Делай” (см. 4.2.2 и 5.1).</p>
<p><b>Реакция</b></p> <p>Участники должны действовать своевременно и сообщать, чтобы предотвращать, выявлять и реагировать на инциденты в безопасности.</p>	<p>Частично функция мониторинга выполняется на этапе “Проверяй” (см. 4.2.3 и с 6 по 7.3), а функция реагирования – на этапе “Действуй” (см. 4.2.4 и с 8.1 по 8.3). Также они могут соответствовать некоторым положениям этапов “Проверяй” и “Планируй”.</p>
<p><b>Оценка риска</b></p> <p>Участники должны проводить оценку рисков.</p>	<p>Данная функция выполняется на этапе “Планируй” (см. 4.2.1), функция переоценки риска – на этапе “Проверяй” (см 4.2.3 и с 6 по 7.3).</p>
<p><b>Моделирование и внедрение безопасности</b></p> <p>Участники должны рассматривать безопасность как весьма важный элемент информационных систем и сетей.</p>	<p>После завершения этапа оценки риска в целях сокращения риска выбираются средства управления, что соответствует этапу “Планируй” (см. 4.2.1). Последующий этап “Делай” (см. 4.2.2 и 5.2) характеризуется внедрением и практическим использованием этих средств управления.</p>
<p><b>Менеджмент безопасности</b></p> <p>Участники должны использовать всеобъемлющую концепцию менеджмента безопасности.</p>	<p>Управление риском – процесс, включающий предотвращение, выявление и реагирование на инциденты, постоянную поддержку, проверку и аудит. Все эти аспекты затронуты на этапах “Планируй”, “Делай”, “Проверяй” и “Действуй”.</p>
<p><b>Переоценка</b></p> <p>Участники должны пересматривать и проводить переоценку безопасности информационных систем и сетей, и в соответствии с этим модифицировать политики безопасности, технологии, методы оценок и процедуры.</p>	<p>Функция переоценки информационной безопасности выполняется на этапе “Проверяй” (см. 4.2.3 и с 6 по 7.3), на котором необходимо проводить регулярные проверки эффективности системы менеджмента информационной безопасности, а процесс совершенствования соответствует этапу “Действуй” (см. 4.2.4 и с 8.1 по 8.3).</p>

Приложение С  
(информативное)  
**Связь между стандартами МС 9001:2000, МС 14001:2004 и  
данным  
Международным Стандартом**

Таблица С.1 демонстрирует связь между стандартами МС 9001:2000, МС 14001:2004 и данным Международным Стандартом.

**Таблица С.1 — Связь между стандартами МС 9001:2000, МС 14001:2004 и данным Международным Стандартом**

<b>Данный Международный Стандарт</b>	<b>МС 9001:2000</b>	<b>МС 14001:2004</b>
<b>0 Введение</b> 0.1 Общие положения 0.2 Концепция процесса менеджмента 0.3 Совместимость с другими системами менеджмента	<b>0 Введение</b> 0.1 Общие положения 0.2 Концепция процесса менеджмента 0.3 Связь со стандартом МС 9004 0.4 Совместимость с другими системами менеджмента	<b>0 Введение</b>
<b>1 Обзор</b> 1.1 Общие положения 1.2 Применение	<b>1 Обзор</b> 1.1 Общие положения 1.2 Применение	<b>1 Обзор</b>
<b>2 Нормативные ссылки</b>	<b>2 Нормативные ссылки</b>	<b>2 Нормативные ссылки</b>
<b>3 Термины и определения</b>	<b>3 Термины и определения</b>	<b>3 Термины и определения</b>
<b>4 Система менеджмента информационной безопасности</b> 4.1 Общие требования 4.2 Создание и менеджмент СМИБ 4.2.1 Создание СМИБ	<b>4 Система менеджмента качества</b> 4.1 Общие требования	<b>4 Требования EMS</b> 4.1 Общие требования
4.2.2 Внедрение и использование СМИБ 4.2.3 Мониторинг и проверка СМИБ	8.2.3 Мониторинг и оценка технологических процессов 8.2.4 Мониторинг и системы оценки продукции	4.4 Внедрение и использование 4.5.1 Мониторинг и системы оценок
4.2.4 Поддержка и совершенствование СМИБ		
4.3 Требования обеспечения документацией 4.3.1 Общие положения 4.3.2 Контроль документов 4.3.3 Контроль записей	4.2 Требования обеспечения документацией 4.2.1 Общие положения 4.2.2 Руководство по определению качества 4.2.3 Контроль документов 4.2.4 Контроль записей	4.4.5 Контроль документов 4.5.4 Контроль записей
<b>5 Обязанности руководства</b> 5.1 Обязательства руководства	<b>5 Обязанности руководства</b> 5.1 Обязательства руководства 5.2 Ориентация на покупателя 5.3 Политика качества 5.4 Планирование 5.5 Ответственность, полномочия, и связи	4.2 Экологическая политика 4.3 Планирование
5.2 Управление трудовыми ресурсами 5.2.1 Обеспечение кадрами	<b>6 Управление трудовыми ресурсами</b> 6.1 Обеспечение кадрами	

Данный Международный Стандарт	МОС 9001:2000	МОС 14001:2004
5.2.2 Обучение, информированность и компетентность	6.2 Кадры 6.2.2 Компетентность, информированность и обучение 6.3 Инфраструктура 6.4 Рабочая обстановка	4.4.2 Компетентность, обучение и информированность
<b>6 Внутренние аудиты СМИБ</b>	8.2.2 Внутренний Аудит	4.5.5 Внутренний аудит
<b>7 Проверка управления СМИБ</b> 7.1 Общие положения 7.2 Входные данные для проверки 7.3 Выходные данные проверки	<b>5.6 Проверка управления</b> 5.6.1 Общие положения 5.6.2 Входные данные для проверки 5.6.3 Выходные данные проверки	<b>4.6 Проверка управления</b>
<b>8 Совершенствование СМИБ</b> 8.1 Постоянное совершенствование	<b>8.5 Совершенствование</b> 8.5.1 Постоянное совершенствование	
8.2 Корректирующие меры	8.5.3 Корректирующие меры	4.5.3 Мероприятия по устранению несогласованностей, а также корректирующие и превентивные мероприятия
8.3 Превентивные мероприятия	8.5.3 Превентивные мероприятия	
<b>Приложение А Цели и средства управления</b>  <b>Приложение В Принципы ОЭСР и данного Международного Стандарта</b>  <b>Приложение С Связь между стандартами МОС 9001:2000, МОС 14001:2004 и данным Международным Стандартом</b>	<b>Приложение А Связь между стандартами МОС 9001:2000 и МОС 14001:1996</b>	<b>Приложение А Руководство по использованию данного Международного Стандарта</b>  <b>Приложение В Связь между стандартами МОС 14001:2004 и МОС 9001:2000</b>

## Библиография

### Изданные Стандарты

- [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 издания

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