ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ГОСТ Р 57640— 2017/ ISO/IEC TS 33052:2016**

## Информационные технологии

# ЭТАЛОННАЯ МОДЕЛЬ ПРОЦЕССА (ЭМП) ДЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

(ISO/IEC TS 33052:2016, IDT)

Издание официальное

Москва
Стандартинформ
2017

## Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 5 сентября 2017 г. № 1015-ст

4 Настоящий стандарт идентичен международному документу ISO/IEC TS 33052:2016 «Информационные технологии. Эталонная модель процесса (ЭМП) для управления информационной безопасностью» (ISO/IEC TS 33052:2016 «Information technology — Process reference model (PRM) for information security management», IDT).

ISO/IEC TS 33052 разработан подкомитетом ПК 7 «Системная и программная инженерия» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК).

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

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые положения международного документа, указанного в пункте 4, могут являться объектом патентных прав. ИСО и МЭК не несут ответственности за идентификацию подобных патентных прав

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)*

## Содержание

## Введение

Цель настоящего стандарта состоит в том, чтобы облегчить разработку модели оценки процесса (МОП), приведенной в ИСО/МЭК 33072.

ИСО/МЭК 33002 устанавливает требования для осуществления оценки процесса. ИСО/МЭК 33020 описывает шкалу измерений для оценки характеристик качества с точки зрения возможностей процесса. ИСО/МЭК 33001 определяет понятия и терминологию, используемые для оценки процесса.

Эталонная модель процесса (ЭМП) является моделью, включающей в себя определения процессов, описанных в терминах цели и результатов, совместно с архитектурой, определяющей отношения между процессами. При использовании ЭМП на практике могут потребоваться дополнительные элементы, отвечающие окружающей среде и обстоятельствам.

ЭМП, определенная в настоящем стандарте, описывает ряд процессов, включая процессы системы управления информационной безопасностью (СУИБ), приведенные в ИСО/МЭК 27001. Каждый процесс ЭМП описан в терминах цели и результатов и обеспечивает прослеживаемость требований. ЭМП не пытается разместить процессы в заданной среде и не предопределяет уровень возможностей процесса, необходимых для выполнения требований ИСО/МЭК 27001. ЭМП не предназначена для аудита оценки соответствия или использования в качестве эталонного руководства по реализации процесса.

Соотношение между стандартами ИСО/МЭК 24774, ИСО/МЭК 27001, ИСО/МЭК 33002, ИСО/МЭК 33004, ИСО/МЭК 33020, ИСО/МЭК TS 33052 и ИСО/МЭК TS 33072 приведено на рисунке 1.

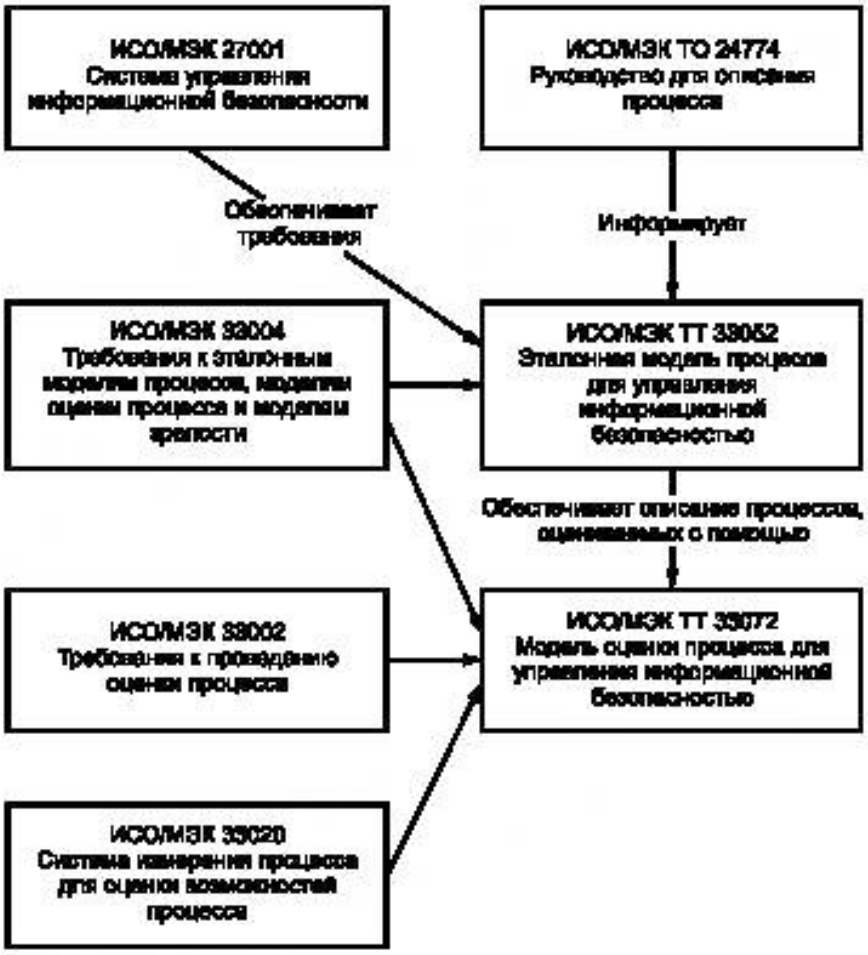


Рисунок 1 — Соотношение между соответствующими стандартами

Любая организация может определить процессы с какими-либо дополнительными элементами, адаптируясь к определенной среде и обстоятельствам. Некоторые процессы охватывают общие аспекты управления в организации. Эти процессы должны быть определены так, чтобы соответствовать требованиям ИСО/МЭК 27001.

ЭМП не обеспечивает предоставление свидетельств, требуемых ИСО/МЭК 27001. ЭМП не определяет взаимодействие между процессами.

Описания процессов в рамках ЭМП для управления информационной безопасностью приведены в разделе 5. Приложение А обеспечивает положения в соответствии с ИСО/МЭК 33002.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

# ЭТАЛОННАЯ МОДЕЛЬ ПРОЦЕССА (ЭМП) ДЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Information technology. Process reference model (PRM) for information security management

Дата введения — 2018—09—01

## 1 Область применения

В настоящем стандарте определена эталонная модель процесса (ЭМП) для управления информационной безопасностью. Архитектура модели определяет архитектуру процесса для области применения и включает ряд процессов, каждый из которых описан в терминах цели и результатов процесса.

## 2 Нормативные ссылки

В настоящем стандарте применены следующие нормативные ссылки. Для датированных документов используются только указанные издания. Для недатированных документов используются последние издания с учетом внесенных в них изменений.

ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements (Информационные технологии. Методы безопасности. Системы управления информационной безопасностью. Требования)

ISO/IEC 33001, Information technology — Process assessment — Concepts and terminology (Информационные технологии. Оценка процесса. Понятия и терминология)

## 3 Термины и определения

В настоящем стандарте применены термины и соответствующие определения по ИСО/МЭК 27001 и ИСО/МЭК 33001.

## 4 Краткий обзор ЭМП

Структура ЭМП, применяемая для поддержки управления информационной безопасностью, приведена в настоящем разделе. ЭМП включает процессы, которые могут существовать в контексте системы управления у поставщика услуг.

Процессы, определенные согласно требованиям ИСО/МЭК 27001, приведены на рисунке 2.

Издание официальное


Рисунок 2 — Процессы в ЭМП

## 5 Описания процесса

### 5.1 Введение

Каждый процесс в ЭМП может быть описан с помощью следующих элементов:

a) идентификатора процесса: каждый процесс, принадлежащий группе, идентифицируется с использованием идентификатора процесса, состоящего из сокращенного названия группы и последующего номера процесса в этой группе;

b) названия: название процесса — короткая фраза, описывающая область процесса, идентифицируя основной интерес процесса, и отличающая его от других процессов в рамках ЭМП;

c) контекста: краткий обзор для каждого процесса, описывающий намеченный контекст применения процесса;

d) цели процесса: некий высокий уровень достижений в результате выполнения процесса;

e) выходов (выходных результатов): наблюдаемый результат успешного достижения цели процесса. Результаты являются оцениваемыми, материальными, техническими или деловыми, достигаемыми с помощью процесса. Выходы являются наблюдаемыми и подлежат оценке;

f) прослеживаемости требований: результаты основаны на требованиях ИСО/МЭК 27001. Ссылки идентифицируют применимые подразделы ИСО/МЭК 27001, заголовок подраздела и поддерживаемые результаты.

Все записи в ряду прослеживаемых требований в подразделах с 5.2 по 5.27 заканчиваются числами в квадратных скобках, т. е. [n]. Каждое число в квадратных скобках — это ссылка на пронумерованный результат. Эти результаты непосредственно связаны с требованиями ИСО/МЭК 27001.

Некоторые выходные результаты отражаются в квадратных скобках. Они только косвенно связаны с требованиями ИСО/МЭК 27001. Ни одна из записей в ряду прослеживаемых требований не ссылается на результаты в квадратных скобках. Эти дополнительные результаты были включены постольку, поскольку считаются необходимыми для данного типа ЭМП как основы МОП (ИСО/МЭК TS 33072). С этими дополнительными результатами процесс является полным, и цель процесса может быть достигнута.

### 5.2 ORG.1 Управление активами

| Идентификатор процесса | ORG.1 | |
|---|---|---|
| Название | Управление активами | |
| Цель | Цель процесса состоит в том, чтобы установить и поддерживать целостность всех идентифицированных активов продукции | |
| Контекст | Этот процесс связан с установлением и поддержанием идентичности продуктов и их конфигурационной информации для обеспечения эффективного контроля продукции. Область активов может включать в себя физические активы (например, инфраструктуру, аппаратные средства, программные средства) и нематериальные активы (например, интеллектуальную собственность) | |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Идентифицируются объекты, требующие управления активами.<br>2 Классифицируются объекты активов.<br>3 Инвентаризируются активы.<br>4 [Определяется статус активов].<br>5 Контролируются изменения активов, находящихся под управлением | |
| Прослеживаемость требований | 27001 2ED A.08.1.1 | Инвентаризация активов [1, 3, 5] |
| | 27001 2ED A.08.2.1 | Классификация информации [2] |
| | 27001 2ED A.08.3.2 | Утилизация носителей информации [5] |
| | 27001 2ED A.08.3.3 | Физическое перемещение носителей информации [5] |

### 5.3 TEC.01 Управление возможностями

| Идентификатор процесса | TEC.01 |
|---|---|
| Название | Управление возможностями |
| Цель | Цель процесса состоит в обеспечении гарантий того, что у организации имеются возможности для удовлетворения текущим и будущим системным требованиям |
| Контекст | Этот процесс гарантирует достаточность ресурсов и возможностей для удовлетворения согласованным требованиям, эффективным по стоимости и времени. Процесс позволяет поставщику услуг обеспечить достаточные ресурсы согласованного выполнения услуг и достижения целей на должном уровне |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 [Определяются текущая и будущая возможности и требования для удовлетворения потребностей].<br>2 [Обеспечиваются возможности для удовлетворения текущих возможностей и потребностей].<br>3 Контролируется использование возможностей, анализируется и осуществляется настройка для удовлетворения потребностей.<br>4 [Подготавливаются возможности для удовлетворения будущих возможностей и потребностей] |
| Прослеживаемость требований | 27001 2ED A.12.1.3 Управление возможностями [3] |

### 5.4 TEC.02 Управление изменениями

| Идентификатор процесса | TEC.02 |
|---|---|
| Название | Управление изменениями |
| Цель | Цель процесса состоит в том, чтобы обеспечить направленность всех действий, связанных с изменениями, касающимися продукции, услуг, процессов и систем, используемыми для производства продукции или оказания услуг |
| Контекст | Изменения, касающиеся продукции, услуг и систем, их применению и инфраструктуры, планируются и управляются для обеспечения гарантий по времени выполнения без ненужных сбоев |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 [Классифицируются запросы на изменения].<br>2 Анализируются и оцениваются заявки на изменения с использованием определенных критериев.<br>3 [Анализируются и оцениваются изменения с использованием определенных критериев].<br>4 [Если изменения принимаются, они реализуются] |
| Прослеживаемость требований | 27001 2ED A.15.2.2 Управление изменениями в услугах поставщика [2] |

### 5.5 COM.01 Управление связью

| Идентификатор процесса | COM.01 |
|---|---|
| Название | Управление связью |
| Цель | Цель процесса состоит в том, чтобы предоставлять своевременную и точную информационную продукцию для поддержки эффективной связи и принятия решений |
| Контекст | Этот процесс представляет собой сосредоточение всех действий по связи в процессах систем управления |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Формируется информационное содержание в терминах определенных потребностей связи и требований.<br>2 Определяются стороны для связи.<br>3 Определяется сторона, ответственная за связь.<br>4 Определяются события, которые требуют действий по связи.<br>5 Выбирается канал связи.<br>6 Доводится до заинтересованных сторон информационная продукция |
| Прослеживаемость требований | 27001 2ED 05.1 Лидерство и обязательства [6]<br>27001 2ED 05.2 Политика [6]<br>27001 2ED 05.3 Организационные функции, ответственность и полномочия [6]<br>27001 2ED 06.2 Цели в области информационной безопасности и планирование их достижения [6]<br>27001 2ED 07.4 Связь [1—5]<br>27001 2ED 09.2 Внутренний аудит [6]<br>27001 2ED A.05.1.1 Политики обеспечения информационной безопасности [6]<br>27001 2ED A.06.1.3 Контакт с полномочными органами [2]<br>27001 2ED A.06.1.4 Контакты с профессиональными сообществами [2]<br>27001 2ED A.07.2.3 Дисциплинарные меры [6]<br>27001 2ED A.07.3.1 Освобождение от обязанностей или их изменение [6] |

### 5.6 TEC.03 Управление конфигурацией

| Идентификатор процесса | TEC.03 | |
|---|---|---|
| Название | Управление конфигурацией | |
| Цель | Цель процесса состоит в том, чтобы определять, контролировать, регистрировать, отслеживать, делать отчеты и проверять все идентифицированные компоненты продукции/услуг | |
| Контекст | Этот процесс позволяет установить и поддержать целостность компонентов продукции/услуг для обеспечения их эффективного контроля | |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 [Определяются объекты, требующие управления конфигурацией].<br>2 [Определяется статус объектов конфигурации и модификаций].<br>3 Контролируются изменения по объектам под управлением конфигурацией.<br>4 [Гарантируется целостность систем, продукции/услуг и компонентов продукции/услуг].<br>5 [Контролируется конфигурация выпущенных объектов] | |
| Прослеживаемость требований | 27001 2ED A.14.2.4 | Ограничения на изменения в пакетах программ [3] |
| | 27001 2ED A.14.3.1 | Защита данных для тестирования [3] |

### 5.7 COM.02 Управление документацией

| Идентификатор процесса | COM.02 | |
|---|---|---|
| Название | Управление документацией | |
| Цель | Цель процесса состоит в том, чтобы обеспечить своевременное предоставление соответствующей полной, достоверной и, если необходимо, конфиденциальной зарегистрированной информации согласно ее назначению | |
| Контекст | Этот процесс обеспечивает меры для того, чтобы запрошенная задокументированная информация (например, процедуры, инструкции и шаблоны) была доступна согласно ее назначению для достижения целей информационной безопасности | |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Определяется документируемая информация, которая подлежит управлению.<br>2 Определяются формы регистрируемого представления информации.<br>3 Становится известным статус содержания регистрируемой информации.<br>4 Документируемая информация является обновляемой, полной и достоверной.<br>5 Документируемая информация выпускается согласно определенным критериям.<br>6 Документируемая информация становится доступной для назначенных сторон.<br>7 Документируемая информация архивируется или уничтожается согласно установленным требованиям | |
| Прослеживаемость требований | 27001 2ED 04.3 | Определение области СУИБ [1] |
| | 27001 2ED 05.2 | Политика [1, 6] |
| | 27001 2ED 06.1.2 | Оценка рисков нарушения информационной безопасности [1] |
| | 27001 2ED 06.1.3 | Реакция на риски нарушения информационной безопасности [1, 5] |
| | 27001 2ED 06.2 | Цели в области информационной безопасности и планирование их достижения [1, 3] |
| | 27001 2ED 07.2 | Компетентность [1] |

| | | |
|---|---|---|
| | 27001 2ED 07.5.2 | Создание и обновление [2, 5] |
| | 27001 2ED 07.5.3 | Контроль зарегистрированной информации [2—4, 6, 7] |
| | 27001 2ED 08.1 | Эксплуатационное планирование и контроль [7] |
| | 27001 2ED 08.3 | Реакция на риски нарушения информационной безопасности [1, 5] |
| | 27001 2ED 09.1 | Контроль, измерения, анализ и оценка [1] |
| | 27001 2ED 09.2 | Внутренний аудит [1] |
| | 27001 2ED 09.3 | Анализ управления [1] |
| | 27001 2ED 10.1 | Несоответствия и корректирующие действия [1] |
| | 27001 2ED A.05.1.1 | Политика обеспечения информационной безопасности [5, 6] |
| | 27001 2ED A.08.1.3 | Надлежащее использование активов [1] |
| | 27001 2ED A.09.1.1 | Политика контроля доступа [1] |
| | 27001 2ED A.12.1.1 | Зарегистрированные рабочие процедуры [1, 6] |
| | 27001 2ED A.12.4.1 | Регистрация событий [1] |
| | 27001 2ED A.13.2.4 | Соглашения о конфиденциальности или неразглашении [1] |
| | 27001 2ED A.14.2.5 | Принципы безопасной системной инженерии [1, 3] |
| | 27001 2ED A.15.1.1 | Политика информационной безопасности в отношениях с поставщиками [1, 3] |
| | 27001 2ED A.16.1.5 | Реагирование на инциденты нарушения информационной безопасности [1] |
| | 27001 2ED A.16.1.7 | Сбор свидетельств [1] |
| | 27001 2ED A.17.1.2 | Обеспечение непрерывности информационной безопасности [1, 3] |
| | 27001 2ED A.18.1.1.01 | Применяемые законодательные и нормативные требования [1,3] |
| | 27001 2ED A.18.1.1.02 | Применяемые контрактные требования [1, 3] |
| | 27001 2ED A.18.1.3 | Защита записей [4] |

### 5.8 ORG.2 Управление оборудованием

| Идентификатор процесса | ORG.2 |
|---|---|
| Название | Управление оборудованием |
| Цель | Цель процесса — гарантировать целостность функционирования и поведения оборудования и связанных с ним программных средств |
| Контекст | Этот процесс определяет действия, которые будут предприняты для защиты оборудования от изменений по установке (т. е. проверка) или изменений в окружающей среде, которые могут привести к сбою в параметрах установки |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Производится установка оборудования таким образом, чтобы минимизировать риск ущерба среде и иного ущерба.<br>2 Гарантируется непрерывность обеспечения услуг для оборудования. |

| | |
|---|---|
| | 3 Оборудование обслуживается таким образом, чтобы гарантировать его длительную пригодность и целостность.<br>4 Оборудование управляется на местах, чтобы гарантировать целостность функционирования.<br>5 Обеспечивается целостность информации после технического обслуживания оборудования.<br>6 Контролируется перемещение оборудования |
| Прослеживаемость требований | 27001 2ED A.11.2.1 Размещение и защита оборудования [1]<br>27001 2ED A.11.2.2 Поддерживающие утилиты [2]<br>27001 2ED A.11.2.3 Защита кабельных сетей [1]<br>27001 2ED A.11.2.4 Обслуживание оборудования [3]<br>27001 2ED A.11.2.5 Перемещение активов [6]<br>27001 2ED A.11.2.6 Защита оборудования и активов вне территории [4]<br>27001 2ED A.11.2.7 Безопасная утилизация или повторное использование оборудования [5]<br>27001 2ED A.13.1.1 Средства управления сетями [3] |

### 5.9 ORG.3 Управление персоналом в период занятости

| Идентификатор процесса | ORG.3 |
|---|---|
| Название | Управление персоналом в период занятости |
| Цель | Цель процесса состоит в том, чтобы предотвратить угрозы информационной безопасности со стороны персонала перед наймом, во время работы и по ее завершению |
| Контекст | Этот процесс обращается к предосторожностям в области безопасности, связанным с работой персонала. Эти предосторожности касаются действий персонала до начала работы, в период работы и после расторжения контракта |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Определяются роли и обязанности служащих, подрядчиков и пользователей, имеющих отношение к третьей стороне.<br>2 Принимаются перспективные работники в соответствии с определенными законами, инструкциями и этикой, согласно профессиональным требованиям с учетом осознанных рисков.<br>3 Устанавливается согласие принимаемых работников со сроками и условиями трудового контракта.<br>4 Руководствуются сроками и условиями занятости.<br>5 [Служащие применяют соответствующие организационные политики и процедуры согласно их рабочим функциям].<br>6 Применяются дисциплинарные меры к служащим, которые нарушили согласованные условия контракта.<br>7 Определяются обязанности по завершению или изменению условий контракта.<br>8 По завершении контракта служащие возвращают организации все активы, находившиеся в их владении.<br>9 Доступ служащего к информационным ресурсам прекращается после завершения контракта |
| Прослеживаемость требований | 27001 2ED 07.1.1 Предварительная проверка [2]<br>27001 2ED 07.1.2 Условия трудового соглашения [1, 3]<br>27001 2ED 07.2.1 Ответственность руководства [4] |

| | | |
|---|---|---|
| | 27001 2ED 07.2.3 | Дисциплинарные меры [6] |
| | 27001 2ED 07.3.1 | Освобождение от обязанностей или их изменение [7] |
| | 27001 2ED 08.1.4 | Возврат активов [8] |
| | 27001 2ED 09.2.6 | Отмена или изменение прав доступа [9] |
| | 27001 2ED 09.3.1 | Использование секретной информации по аутентификации [3] |

### 5.10 COM.03 Управление человеческими ресурсами

| Идентификатор процесса | COM.03 | |
|---|---|---|
| Название | Управление человеческими ресурсами | |
| Цель | Цель процесса состоит в обеспечении организации необходимыми человеческими ресурсами и поддержании их компетентности на уровне, совместимом с деловыми потребностями | |
| Контекст | Этот процесс состоит в определении и разработке компетентности людей относительно их действий и потребностей организационного процесса | |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Определяются компетентности, требуемые организации для производства продукции и услуг.<br>2 Осуществляется обучение или наем с нужным уровнем компетентности, чтобы заполнить выявленные пробелы компетентности.<br>3 Демонстрируются каждым работником понимание роли и действий в достижении целей организации в производстве продукции и услуг | |
| Прослеживаемость требований | 27001 2ED 07.2 | Компетентность [1—3] |
| | 27001 2ED 07.3 | Осведомленность [3] |
| | 27001 2ED A.07.2.2 | Осведомленность, образование и обучение в сфере информационной безопасности [3] |

### 5.11 COM.04 Улучшения

| Идентификатор процесса | COM.04 | |
|---|---|---|
| Название | Улучшения | |
| Цель | Цель процесса состоит в непрерывном совершенствовании системы управления, ее процессов и продукции | |
| Контекст | Этот процесс позволяет организации усовершенствовать систему управления, ее процессы, продукцию и услуги. Этот процесс включает в себя определение, оценку, утверждение, установление приоритетов управления, измерение и обзор улучшений | |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Определяются возможности улучшения.<br>2 [Производится оценка возможности улучшения по определенным критериям].<br>3 [Улучшения располагаются по приоритетам].<br>4 [Реализуются улучшения].<br>5 [Оценивается эффективность реализованных улучшений] | |
| Прослеживаемость требований | 27001 2ED 09.3 | Анализ управления [1] |

### 5.12 TEC.04 Управление инцидентами

| Идентификатор процесса | TEC.04 |
|---|---|
| Название | Управление инцидентами |
| Цель | Цель процесса — определять и разрешать события в области информационной безопасности и инциденты в пределах согласованных уровней услуг |
| Контекст | Цель управления инцидентами состоит в том, чтобы восстановить услуги в пределах согласованных уровней их реализации. При этом ориентируются на сокращение продолжительности и последствий простоев в работе и клиентских аспектах, а не на установление первопричин инцидентов |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Определяются инциденты.<br>2 Классифицируются, располагаются по приоритетам и анализируются инциденты.<br>3 Разрешаются и закрываются инциденты.<br>4 [Делается отчет по инцидентам, инциденты учитываются в соответствии с согласованными уровнями услуг] |
| Прослеживаемость требований | 27001 2ED 16.1.2 Отчетность о событиях, связанных с информационной безопасностью [1]<br>27001 2ED 16.1.3 Отчетность об уязвимостях в области информационной безопасности [1]<br>27001 2ED 16.1.4 Оценки и решения по событиям информационной безопасности [2]<br>27001 2ED 16.1.5 Реагирование на инциденты нарушения информационной безопасности [3] |

### 5.13 ORG.4 Инфраструктура и рабочая среда

| Идентификатор процесса | ORG.4 |
|---|---|
| Название | Инфраструктура и рабочая среда |
| Цель | Цель процесса состоит в обеспечении приемлемой инфраструктуры и услуг для проектов, чтобы поддержать цели организации и проектов в их жизненных циклах |
| Контекст | Инфраструктура охватывает физические элементы, которые связаны с физическим оборудованием, где могут быть размещены люди. Рабочая среда относится к мерам в пределах инфраструктуры, которые облегчают и применяют эффективные взаимодействия и действия людей |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Определяются требования к инфраструктуре и рабочей среде, чтобы поддерживать процессы.<br>2 Определяются права доступа к информационным ресурсам.<br>3 [Определяются инфраструктура и элементы рабочей среды].<br>4 [Приобретаются и вводятся в действие инфраструктура и элементы рабочей среды].<br>5 Инфраструктура и рабочая среда управляются и поддерживаются.<br>6 Контролируется доступ к информационным ресурсам.<br>7 Информационные ресурсы защищаются от злоупотреблений |
| Прослеживаемость требований | 27001 2ED A.09.1.2 Доступ к сетям и сетевым службам [6]<br>27001 2ED A.09.2.3 Управление привилегированными правами доступа [6]<br>27001 2ED A.09.2.5 Пересмотр прав доступа пользователей [6]<br>27001 2ED A.09.4.1 Ограничение доступа к информации [2] |

| | | |
|---|---|---|
| | 27001 2ED A.09.4.2 | Безопасные процедуры входа в систему [6] |
| | 27001 2ED A.09.4.3 | Система управления паролями [6] |
| | 27001 2ED A.09.4.4 | Использование утилит с привилегированными правами [7] |
| | 27001 2ED A.09.4.5 | Контроль доступа к исходным кодам [6] |
| | 27001 2ED A.11.1.1 | Физический периметр безопасности [1, 5] |
| | 27001 2ED A.11.1.2 | Контроль физического прохода [1] |
| | 27001 2ED A.11.1.3 | Защита офисов, помещений и устройств [1, 5] |
| | 27001 2ED A.11.1.4 | Защита от внешних угроз и угроз природного характера [1, 5] |
| | 27001 2ED A.11.1.6 | Зоны доставки и отгрузки [5] |
| | 27001 2ED A.11.2.8 | Оборудование пользователя, находящееся без присмотра [5] |
| | 27001 2ED A.12.1.4 | Разделение среды разработки, тестирования и эксплуатации [2] |
| | 27001 2ED A.12.4.1 | Регистрация событий [7] |
| | 27001 2ED A.12.4.2 | Защита регистрируемой информации [7] |
| | 27001 2ED A.12.4.3 | Журналы действий администратора и оператора [6] |
| | 27001 2ED A.12.4.4 | Синхронизация времени [1] |
| | 27001 2ED A.12.6.1 | Управление техническими уязвимостями [7] |
| | 27001 2ED A.13.1.2 | Безопасность сетевых услуг [1] |
| | 27001 2ED A.13.1.3 | Разделение в сетях [2] |
| | 27001 2ED A.13.2.3 | Электронные сообщения [7] |
| | 27001 2ED A.14.1.3 | Защита транзакций прикладных услуг [7] |
| | 27001 2ED A.14.2.6 | Безопасная среда разработки [1] |
| | 27001 2ED A.18.1.4 | Конфиденциальность и защита персональных данных [7] |
| | 27001 2ED A.18.1.5 | Регламентация применения криптографических методов [7] |

### 5.14 COM.05 Внутренний аудит

| Идентификатор процесса | COM.05 |
|---|---|
| Название | Внутренний аудит |
| Цель | Цель процесса — независимое определение соответствия системы управления, услуг и процессов требованиям, политике, планам и соглашениям установленным способом |
| Контекст | Этот процесс включает в себя проведение аудитов с тем, чтобы независимо определить, соответствуют ли система управления и деловые процессы требованиям, установленным организацией |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Определяются область и цель каждого аудита.<br>2 Гарантируются объективность и беспристрастность проведения аудита и выбора аудиторов.<br>3 Определяется соответствие отобранных услуг, продукции и процессов требованиям, планам и соглашениям |

| | | |
|---|---|---|
| Прослеживаемость требований | 27001 2ED 09.2 | Внутренний аудит [1—3] |
| | 27001 2ED A.15.2.1 | Мониторинг и анализ услуг поставщика [3] |
| | 27001 2ED A.18.2.1 | Независимый анализ информационной безопасности [3] |
| | 27001 2ED A.18.2.2 | Соответствие политикам безопасности и стандартам [3] |
| | 27001 2ED A.18.2.3 | Анализ технического соответствия [1] |

### 5.15 TOP.1 Лидерство

| Идентификатор процесса | TOP.1 | |
|---|---|---|
| Название | Лидерство | |
| Цель | Цель процесса — направить организацию на достижение ее видения, назначения, стратегии и целей путем определения и реализации системы управления, политики и целей системы управления | |
| Контекст | Этот процесс состоит в определении области применения системы управления, а также политики и целей | |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Понимается и анализируется среда организации, включая ожидания ее заинтересованных сторон.<br>2 Определяется область действий системы управления с учетом среды организации.<br>3 Определяется политика системы управления и цели.<br>4 Определяются система управления и функциональная стратегия процесса.<br>5 Демонстрируются обязательства и лидерство относительно системы управления | |
| Прослеживаемость требований | 27001 2ED 04.1 | Понимание организации и ее среды [1] |
| | 27001 2ED 04.2 | Понимание потребностей и ожиданий заинтересованных сторон [1] |
| | 27001 2ED 04.3 | Определение области применения СУИБ [2] |
| | 27001 2ED 04.4 | СУИБ [4] |
| | 27001 2ED 05.1 | Лидерство и обязательства [5] |
| | 27001 2ED 05.2 | Политика [3] |
| | 27001 2ED 06.2 | Цели в области информационной безопасности и планирование их достижения [3] |
| | 27001 2ED 07.5.1 | Общее [4] |
| | 27001 2ED 07.5.3 | Управление документируемой информацией [4] |
| | 27001 2ED 08.1 | Эксплуатационное планирование и управление [4] |
| | 27001 2ED 10.2 | Непрерывное улучшение [4] |
| | 27001 2ED A.05.1.1 | Политика обеспечения информационной безопасности [3] |

### 5.16 COM.06 Анализ управления

| Идентификатор процесса | COM.06 |
|---|---|
| Название | Анализ управления |
| Цель | Цель процесса — оценить работу системы управления, определить и принять решения относительно потенциальных улучшений |

| | |
|---|---|
| Контекст | Этот процесс проверяет систему управления через запланированные интервалы с тем, чтобы гарантировать ее непрерывную пригодность, адекватность и эффективность. Анализ может включать любое понимание, располагающееся в области применения: от организации в целом ниже к отдельному процессу, его выходным результатам и поставляемой продукции. Принимаются во внимание результаты аудитов, соответствие процессов требованиям к продукции, услугам, отчетам, инцидентам, ставшим известными ошибкам, рискам, предложениям и обратной связи от заинтересованных сторон |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Устанавливаются цели анализа.<br>2 Оцениваются статус и выполнение действий или процесса в терминах установленных целей.<br>3 Определяются риски, проблемы и возможности для улучшения |
| Прослеживаемость требований | 27001 2ED 09.3 Анализ управления [1—3] |

### 5.17 COM.07 Управление несоответствиями

| Идентификатор процесса | COM.07 |
|---|---|
| Название | Управление несоответствиями |
| Цель | Цель процесса — разрешать несоответствия и устранять их причины, когда это возможно |
| Контекст | Этот процесс устанавливает, что там, где происходят несоответствия, анализ может установить необходимость исправления. Альтернативно исследуются причины несоответствия в целях недопущения возможностей повторного возникновения несоответствий |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Определяются несоответствия.<br>2 Разрешаются и устраняются несоответствия.<br>3 Определяются причины выявленных несоответствий.<br>4 Определяются потребности в действиях для устранения причин несоответствий.<br>5 Реализуются выбранные предложения по действиям.<br>6 Подтверждается эффективность изменений для устранения несоответствий |
| Прослеживаемость требований | 27001 2ED 10.1 Несоответствия и корректирующие действия [1—5, 6] |

### 5.18 COM.09 Функциональная реализация и управление

| Идентификатор процесса | COM.09 |
|---|---|
| Название | Функциональная реализация и управление |
| Цель | Цель процесса — развертывание и управление выполнением функциональных и организационных процессов |
| Контекст | Этот процесс состоит в поддержке эффективных, своевременных и качественных ежедневных функций, оптимизирующих распределение ресурсов и выполнение эксплуатационной политики для поддержания общей всесторонней политики и целей компании |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Определяются необходимые функции, ответственность и полномочия.<br>2 Определяются и используются необходимые ресурсы.<br>3 Реализуются действия, необходимые для достижения целей системы управления. |

| | | |
|---|---|---|
| | 4 Анализируются пригодность и эффективность предпринимаемых действий для достижения целей системы управления.<br>5 Корректируются отклонения в случае, если цели не достигаются.<br>6 [Данные собираются и анализируются как основание для того, чтобы понять поведение и продемонстрировать пригодность и эффективность процессов] | |
| Прослеживаемость требований | 27001 2ED 05.3 | Организационные функции, ответственность и полномочия [1] |
| | 27001 2ED 06.1.2 | Оценка рисков нарушения информационной безопасности [3, 4] |
| | 27001 2ED 06.1.3 | Реакция на риски нарушения информационной безопасности [3] |
| | 27001 2ED 07.1 | Ресурсы [2] |
| | 27001 2ED 07.2 | Компетентность [4] |
| | 27001 2ED 08.1 | Эксплуатационное планирование и управление [3-5] |
| | 27001 2ED 09.2 | Внутренний аудит [3, 4] |
| | 27001 2ED A.05.1.2 | Анализ политик информационной безопасности [4] |
| | 27001 2ED A.06.1.1 | Должностные функции и ответственность, связанные с информационной безопасностью [1] |
| | 27001 2ED A.06.2.1 | Политика в отношении мобильных устройств [3] |
| | 27001 2ED A.06.2.2 | Удаленная работа [3] |
| | 27001 2ED A.08.1.3 | Надлежащее использование активов [3] |
| | 27001 2ED A.08.2.2 | Маркировка информации [3] |
| | 27001 2ED A.08.2.3 | Обращение с активами [3] |
| | 27001 2ED A.08.3.1 | Управление съемными носителями [3] |
| | 27001 2ED A.09.1.1 | Политика контроля доступа [4] |
| | 27001 2ED A.09.2.1 | Регистрация и отмена регистрации пользователя [3] |
| | 27001 2ED A.09.2.2 | Предоставление доступа пользователю [3] |
| | 27001 2ED A.09.2.4 | Управление секретной аутентификационной информацией пользователей [3] |
| | 27001 2ED A.10.1.1 | Политика использования криптографических методов защиты [3] |
| | 27001 2ED A.10.1.2 | Управление ключами [3] |
| | 27001 2ED A.11.1.5 | Работа в охраняемых зонах [3] |
| | 27001 2ED A.11.2.9 | Политика чистого стола и чистого экрана [3] |
| | 27001 2ED A.12.1.2 | Управление изменениями [4, 5] |
| | 27001 2ED A.12.2.1 | Меры защиты от вредоносного кода [3] |
| | 27001 2ED A.12.4.1 | Регистрация событий [4] |
| | 27001 2ED A.12.4.3 | Регистрации действий администратора и оператора [4] |
| | 27001 2ED A.12.5.1 | Установка программ в эксплуатируемых системах [3] |

| | | |
|---|---|---|
| | 27001 2ED A.12.6.2 | Ограничения на установку программных средств [3] |
| | 27001 2ED A.12.7.1 | Управление аудитом информационных систем [4] |
| | 27001 2ED A.13.2.4 | Соглашения о конфиденциальности или неразглашении [4] |
| | 27001 2ED A.14.2.3 | Технический обзор применений после операционных изменений платформы [4] |
| | 27001 2ED A.14.2.7 | Разработка, произведенная на стороне [4] |
| | 27001 2ED A.15.2.1 | Контроль и анализ услуг поставщика [4] |
| | 27001 2ED A.16.1.7 | Сбор свидетельств [3] |
| | 27001 2ED A.17.1.2 | Обеспечение непрерывности информационной безопасности [3] |
| | 27001 2ED A.17.1.3 | Верификация, анализ и оценка непрерывности информационной безопасности [4] |
| | 27001 2ED A.17.2.1 | Пригодность услуг обработки информации [3] |
| | 27001 2ED A.18.1.2 | Права интеллектуальной собственности [3] |
| | 27001 2ED A.18.2.1 | Независимый анализ информационной безопасности [4] |
| | 27001 2ED A.18.2.2 | Соответствие политикам и стандартам безопасности [4] |
| | 27001 2ED A.18.2.3 | Анализ технического соответствия [4] |

### 5.19 COM.08 Эксплуатационное планирование

| Идентификатор процесса | COM.08 |
|---|---|
| Название | Эксплуатационное планирование |
| Цель | Цель процесса состоит в определении характеристик всех функциональных и организационных процессов и планировании их выполнения |
| Контекст | Область применения этого процесса включает в себя создание политики, процедур, описаний процесса и планов, требуемых организационными и функциональными процессами организации. Определяются функции и ответственность, связанные с выявляемыми упущениями в бизнес-процессах. Определяются потребности в ресурсах. Описываются методы для мониторинга эффективности процесса |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Определяются потребности процесса и требования.<br>2 [Определяются продукты входа и выхода процесса].<br>3 Определяется совокупность видов деятельности, которые преобразуют входы в выходы.<br>4 [Определяются последовательность и взаимодействие процесса с другими процессами].<br>5 Определяются необходимые компетентности и функции для выполнения процесса.<br>6 Определяются необходимые ресурсы для выполнения процесса.<br>7 Определяются методы для мониторинга эффективности и пригодности процесса.<br>8 Разрабатываются планы относительно развертывания процесса |
| Прослеживаемость требований | 27001 2ED 05.3 Организационные функции, ответственность и полномочия [5]<br>27001 2ED 06.1.1 Общие положения [1, 8]<br>27001 2ED 06.1.2 Оценка рисков нарушения информационной безопасности [1]<br>27001 2ED 06.1.3 Реакция на риски нарушения информационной безопасности [1] |

| | | |
|---|---|---|
| | 27001 2ED 06.2 | Цели в области информационной безопасности и планирование их достижения [1, 5, 6, 7, 8] |
| | 27001 2ED 07.1 | Ресурсы [6] |
| | 27001 2ED 07.2 | Компетентность [5] |
| | 27001 2ED 08.2 | Оценка рисков нарушения информационной безопасности [8] |
| | 27001 2ED 09.1 | Мониторинг, измерение, анализ и оценка [5, 8] |
| | 27001 2ED 09.2 | Внутренний аудит [8] |
| | 27001 2ED 09.3 | Анализ управления [8] |
| | 27001 2ED A.05.1.2 | Анализ политики информационной безопасности [8] |
| | 27001 2ED A.06.1.1 | Должностные функции и ответственность, связанные с информационной безопасностью [5] |
| | 27001 2ED A.06.1.2 | Разделение обязанностей [5] |
| | 27001 2ED A.06.1.5 | Информационная безопасность в управлении проектами [1] |
| | 27001 2ED A.06.2.1 | Политика в отношении мобильных устройств [1] |
| | 27001 2ED A.06.2.2 | Удаленная работа [1,3] |
| | 27001 2ED A.08.1.2 | Владение активами [5] |
| | 27001 2ED A.08.1.3 | Надлежащее использование активов [1] |
| | 27001 2ED A.08.2.2 | Маркировка информации [3] |
| | 27001 2ED A.08.2.3 | Обращение с активами [3] |
| | 27001 2ED A.08.3.1 | Управление съемными носителями [3] |
| | 27001 2ED A.08.3.2 | Утилизация носителей информации[3] |
| | 27001 2ED A.09.1.1 | Политика контроля доступа [1] |
| | 27001 2ED A.09.2.1 | Регистрация и отмена регистрации пользователя [1] |
| | 27001 2ED A.09.2.4 | Управление секретной аутентификационной информацией пользователей [1] |
| | 27001 2ED A.09.2.5 | Анализ прав доступа пользователей [8] |
| | 27001 2ED A.10.1.1 | Политика использования криптографических методов защиты [1] |
| | 27001 2ED A.10.1.2 | Управление ключами [1] |
| | 27001 2ED A.11.1.5 | Работа в охраняемых зонах [3] |
| | 27001 2ED A.11.2.9 | Политика чистого стола и чистого экрана [1] |
| | 27001 2ED A.12.1.1 | Зарегистрированные рабочие процедуры [3] |
| | 27001 2ED A.12.3.1 | Резервное копирование информации [1,8] |
| | 27001 2ED A.12.5.1 | Установка программ в эксплуатируемых системах [3] |
| | 27001 2ED A.12.6.2 | Ограничения на установку программных средств [1] |
| | 27001 2ED A.12.7.1 | Управление аудитом информационных систем [8] |
| | 27001 2ED A.13.2.1 | Политики и процедуры передачи информации [1,3] |
| | 27001 2ED A.13.2.4 | Соглашения о конфиденциальности или неразглашении [1] |
| | 27001 2ED A.14.2.1 | Политика безопасности при разработке [1] |

| | | |
|---|---|---|
| | 27001 2ED A.14.2.2 | Процедуры управления системными изменениями [1] |
| | 27001 2ED A.14.2.5 | Принципы безопасной системной инженерии [1] |
| | 27001 2ED A.14.2.8 | Тестирование безопасности системы [1] |
| | 27001 2ED A.15.1.1 | Политика информационной безопасности в отношениях с поставщиками [1] |
| | 27001 2ED A.15.2.1 | Контроль и анализ услуг поставщика [8] |
| | 27001 2ED A.16.1.1 | Ответственность и процедуры [3,5] |
| | 27001 2ED A.16.1.5 | Реагирование на инциденты нарушения информационной безопасности [3] |
| | 27001 2ED A.16.1.7 | Сбор свидетельств [3] |
| | 27001 2ED A.17.1.2 | Обеспечение непрерывности информационной безопасности [1] |
| | 27001 2ED A.17.1.3 | Верификация, анализ и оценка непрерывности информационной безопасности [8] |
| | 27001 2ED A.18.1.2 | Права интеллектуальной собственности [3] |
| | 27001 2ED A.18.2.1 | Независимый анализ информационной безопасности [8] |
| | 27001 2ED A.18.2.2 | Соответствие политикам безопасности и стандартам [8] |
| | 27001 2ED A.18.2.3 | Анализ технического соответствия [8] |

### 5.20 COM.10 Оценка функционирования

| Идентификатор процесса | COM.10 | |
|---|---|---|
| Название | Оценка функционирования | |
| Цель | Цель процесса состоит в сборе и анализе данных, которые будут использованы для оценки работы системы управления и бизнес-процессов в терминах определенных целей | |
| Контекст | Этот процесс состоит из контроля достижения целей информационной безопасности, а также выполнения функциональных и организационных процессов | |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Определяется контроль функционирования и потребности в измерениях.<br>2 [Определяются показатели функционирования, полученные на основе измерений].<br>3 Определяются методы оценки функционирования по соответствующим показателям.<br>4 [Данные собираются с использованием определенных методов управления функционированием].<br>5 Анализируются собранные данные о функционировании | |
| Прослеживаемость требований | 27001 2ED 06.2 | Цели в области информационной безопасности и планирование их достижения [1] |
| | 27001 2ED 09.1 | Мониторинг, измерение, анализ и оценка [1, 3, 5] |
| | 27001 2ED A.16.1.6 | Извлечение уроков из инцидентов нарушения информационной безопасности [5] |
| | 27001 2ED 06.1.3 | Реакция на риски нарушения информационной безопасности [5] |

### 5.21 TEC.05 Производство продукции/оказание услуг

| Идентификатор процесса | TEC.05 |
|---|---|
| Название | Производство продукции/оказание услуг |
| Цель | Цель процесса — управление пригодностью продукции/услуг для конкретного заказчика |
| Контекст | Этот процесс отвечает за создание целых выпускаемых пакетов — совокупности производимой продукции/оказываемых услуг и связанных компонентов с развертыванием их назначения |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 [Определяется содержание выпуска].<br>2 [Определяется выпуск и приемные критерии].<br>3 [Комплектуется выпуск из элементов продукции/услуги/ системы].<br>4 [Определяются тесты для выпуска].<br>5 Проверяется выпуск на соответствие определенным критериям.<br>6 [Продукция/услуги/системы выпускаются для конкретного заказчика согласно определенным критериям] |
| Прослеживаемость требований | 27001 2ED A.14.2.3 Технический анализ приложений после изменений операционной платформы [5] |

### 5.22 TEC.08 Продукция/услуги/системные требования

| Идентификатор процесса | TEC.08 |
|---|---|
| Название | Продукция/услуги/системные требования |
| Цель | Цель процесса — установление и согласование требований к продукции, услугам и системам |
| Контекст | Этот процесс осуществляет сбор требований для продукции, услуг и систем. Продукция/услуга/система могут быть произведены по инициативе поставщика (произведено по каталогу) или по запросу от одного или более заказчиков (произведено по заказу). Требования могут касаться новых продукции/услуг/систем или изменений к существующим продукции/услугам/системам |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 [Определяются необходимые характеристики и контекст использования продукции/ услуг/систем].<br>2 [Определяются ограничения по решениям для продукции/услуг/систем].<br>3 Определяются требования для продукции/услуг/систем.<br>4 Определяются требования для валидации (аттестации) продукции/ услуг/систем |
| Прослеживаемость требований | 27001 2ED A.14.1.1 Анализ и установление требований по информационной безопасности [3]<br>27001 2ED A.14.1.2 Безопасность прикладных услуг в сетях общего пользования [3]<br>27001 2ED A.14.2.3 Технический анализ приложений после изменений операционной платформы [3]<br>27001 2ED A.14.2.9 Приемочное тестирование системы [4]<br>27001 2ED A.18.1.1.01 Применяемые законодательные и нормативные требования [3]<br>27001 2ED A.18.1.1.02 Применяемые контрактные требования [3] |

### 5.23 COM.11 Управление рисками и возможностями

| Идентификатор процесса | COM.11 |
|---|---|
| Название | Управление рисками и возможностями |
| Цель | Цель процесса — определить, проанализировать, оценить, осуществить реакцию на риски и контролировать риски |
| Контекст | Этот процесс состоит из непрерывной идентификации, оценки риска и реакции на риски и возможности, с которыми сталкивается организация |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Идентифицируются риски.<br>2 Анализируются идентифицированные риски.<br>3 Оцениваются риски по определенным критериям.<br>4 Отбираются риски для выработки реакции по ним.<br>5 Осуществляется реакция на отобранные риски |
| Прослеживаемость требований | 27001 2ED 06.1.1 Общие положения [1]<br>27001 2ED 06.1.2 Оценка рисков нарушения информационной безопасности [1—3]<br>27001 2ED 06.1.3 Реакция на риски нарушения информационной безопасности [4]<br>27001 2ED 08.2 Оценка риска [1]<br>27001 2ED 08.3 Осуществление реакции на риски [5] |

### 5.24 TEC.06 Управление готовностью услуг

| Идентификатор процесса | TEC.06 |
|---|---|
| Название | Управление готовностью услуг |
| Цель | Цель процесса — гарантировать, что согласованный уровень услуг будет удовлетворять требованиям в прогнозируемых обстоятельствах |
| Контекст | Этот процесс ответственен за охрану интересов клиентов и иных заинтересованных сторон, гарантируя, что согласованные услуги отвечают предъявляемым требованиям. Этот процесс включает в себя определение, анализ, планирование, измерение и улучшение всех аспектов готовности услуг |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Определяются требования к готовности услуг.<br>2 [Разрабатывается план обеспечения готовности услуг на основе предъявляемых требований].<br>3 [Проверяется готовность услуг по предъявляемым требованиям].<br>4 [Контролируется готовность услуг].<br>5 [Определяются и анализируются причины неготовности услуг].<br>6 [Предпринимаются корректирующие действия, обращенные к выявленным причинам неготовности услуг] |
| Прослеживаемость требований | 27001 2ED A.17.2.1 Возможность применения средств обработки информации [1] |

### 5.25 TEC.07 Управление непрерывностью услуг

| Идентификатор процесса | TEC.07 | |
|---|---|---|
| Название | Управление непрерывностью услуг | |
| Цель | Цель процесса — гарантировать, что согласованные обязательства по непрерывности услуг будут удовлетворены в пределах согласованных целей, и прерванные услуги будут возобновлены | |
| Контекст | Этот процесс отвечает за охрану интересов клиентов и иных заинтересованных сторон, гарантируя достижение удовлетворенности от согласованных услуг. Этот процесс включает в себя определение, анализ, планирование, измерение и улучшение всех аспектов непрерывности услуг. Процесс уменьшает риски до приемлемого уровня и планирует восстановление услуг в случае их прерывания | |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 Определяются требования непрерывности услуг.<br>2 Планируется непрерывность услуг, отвечающая предъявляемым требованиям].<br>3 Оценивается непрерывность услуг на соответствие требованиям непрерывности.<br>4 [Контролируются изменения в требованиях непрерывности услуг].<br>5 [Обеспечивается непрерывность услуг, в случаях прерывания услуг активизируется план обеспечения непрерывности] | |
| Прослеживаемость требований | 27001 2ED A.17.1.1 | Планирование непрерывности информационной безопасности [1] |
| | 27001 2ED A.17.1.3 | Верификация, анализ и оценка непрерывности информационной безопасности [3] |

### 5.26 ORG.5 Управление поставщиками

| Идентификатор процесса | ORG.5 | |
|---|---|---|
| Название | Управление поставщиками | |
| Цель | Цель процесса — обеспечить, чтобы поставщики продукции, услуг или систем были управляемы и интегрируемы в поставляемые продукцию, услуги или системы, удовлетворяющие согласованным требованиям | |
| Контекст | Поставщики являются участниками поставки продукции, услуг или систем через горизонтальную или вертикальную интеграцию. Процесс гарантирует, что организация устанавливает обязательства с ее поставщиками, которые поддерживают интеграцию и качество продукции или услуг и соглашений между организацией и заказчиками. Последнее обеспечивает верификацию того, что поставщики в свою очередь, в состоянии управлять своими субподрядчиками для удовлетворения их обязательств и договорных требований. Следует учесть, что этот процесс не имеет дела с поставками, например, склада, а также периодических поставок, которые непосредственно не вовлечены в одну или более услуг | |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 [Определяются поставщики].<br>2 Договариваются и определяются с каждым поставщиком о продукции или услугах, которые будут предоставлены.<br>3 [Определяются роли и отношения между поставщиками].<br>4 [Подтверждается способность субподрядчиков отвечать по обязательствам].<br>5 [Контролируются обязательства поставщика по удовлетворению требований].<br>6 [Контролируется работа поставщика по согласованным критериям] | |
| Прослеживаемость требований | 27001 2ED A.13.2.2 | Соглашения по передаче информации [2] |

| | | |
|---|---|---|
| Прослеживаемость требований | 27001 2ED A.15.1.2 | Решение вопросов безопасности в соглашениях с поставщиками [2] |
| | 27001 2ED A.15.1.3 | Цепочка поставок информационно-коммуникационных технологий [2] |

### 5.27 TEC.09 Сохранение и восстановление технических данных

| Идентификатор процесса | TEC.09 |
|---|---|
| Название | Сохранение и восстановление технических данных |
| Цель | Цель процесса состоит в том, чтобы поддерживать и сохранять данные, а также восстанавливать данные с архивных носителей |
| Контекст | Этот процесс обращается к действиям, предпринятым для сохранения электронных данных, а также к действиям, которые в условиях управления восстанавливают данные с архивных носителей |
| Выходные результаты | В результате успешной реализации этого процесса:<br>1 [Определяются требования резервного копирования данных].<br>2 [Определяются требования по восстановлению данных].<br>3 Выполняется резервное копирование данных.<br>4 Выполняется восстановление данных.<br>5 [Сохраняются в условиях управления резервные СМИ].<br>6 [Верифицируются восстановленные данные] |
| Прослеживаемость требований | 27001 2ED A.12.3.1 Резервное копирование информации [3, 4] |

**Приложение А**
**(справочное)**

## Отношения между требованиями к системе управления и эталонной моделью процесса

### А.1 Введение

Общие положения, различия и отношения между СУИБ, используемой согласно ИСО/МЭК 27001, эталонной моделью процесса (ЭМП) настоящего стандарта и оценками характеристик качества процесса приведены в настоящем приложении.

ИСО/МЭК 27001 определяет СУИБ как часть полной системы управления, основанной на риск-ориентированном подходе, установлении, реализации, функционировании, контроле, анализе, сопровождении и улучшении информационной безопасности.

ЭМП используется как основа для того, чтобы развить модели оценки процесса, используемые для оценки возможностей процесса. Последовательное описание процессов в пределах ЭМП и через ЭМП позволяет создать комбинацию процессов из различных ЭМП, которые могут облегчить разработку новых моделей и сравнение моделей между собой.

### А.2 Процессы и модели процесса

#### А.2.1 Процесс в терминах входов и выходов

Для эффективного функционирования организационные процессы определяют и управляют многочисленными связанными действиями. Действия или совокупность действий, использующих ресурсы и входы, которые могут быть преобразованы в выходные результаты, можно рассматривать как процесс. Как правило, результат одного процесса формирует вход к следующему процессу, как приведено на рисунке А.1.

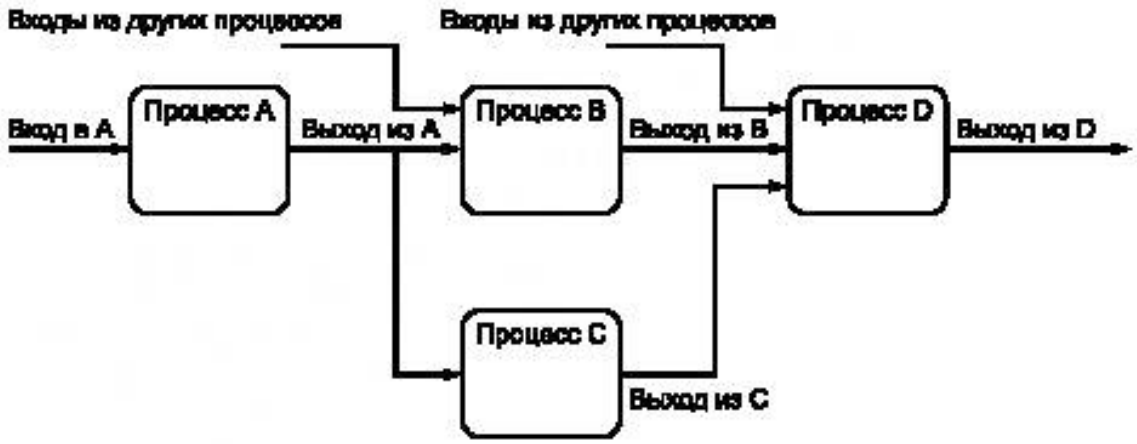


Рисунок А.1 — Процесс, преобразующий входы в выходные результаты

#### А.2.2 Использование ЭМП как основы для понимания возможностей

Понятие «возможность» определено в ИСО 9000 как «способность организации, системы или процесса производить продукцию, которая будет соответствовать требованиям к этой продукции». В ИСО/МЭК 33020 определено, что способность процесса является «характеристикой способности процесса удовлетворять текущей или спроектированной деловой цели».

Следует учитывать то, что представление ИСО 9000 сосредоточено на удовлетворении требований заказчика и результатах процесса, тогда как ИСО/МЭК 33002 сосредотачивается на тех выходных результатах, которые определены как «наблюдаемые результаты процесса». ИСО/МЭК 24774 определяет выходной результат как «наблюдаемый результат успешного достижения цели процесса». Выходные результаты являются измеримыми, материальными, техническими или деловыми результатами, которые достигаются процессом, например результаты, которые используются другими процессами. Выходные результаты являются наблюдаемыми и подлежащими оценке для определенного процесса.

### А.3 Суть требований для системы управления

Требования для систем управления являются базовыми и применимыми к организациям в любой отрасли промышленности или экономическом секторе. ИСО 9000 определяет требования как «потребность или ожидание, которое установлено, предполагается или является обязательным».

### А.4 Отношение требований к ЭМП

ЭМП описывает индивидуальные процессы, тогда как ИСО/МЭК 27001 определяет лишь то, что является частью полной системы управления, основанной на риск-ориентированном подходе, установлении, реализации, функционировании, контроле, анализе, сопровождении и улучшении информационной безопасности.

Процессы иллюстрируются примерами в пределах организации, как правило, в пределах системы управления качеством (например, по ИСО 9001 или ИСО/МЭК 27001).

ИСО/МЭК 27001 устанавливает требования для СУИБ. Некоторые из требований в ИСО/МЭК 27001 являются более широкими, чем требования для индивидуальных процессов, которые могут быть представлены в ЭМП.

Некоторые требования представляют собой общие требования для СУИБ, которые применимы во всех процессах.

Например, ИСО/МЭК 27001 устанавливает требования в 5.1 «Лидерство и обязательства»:

**5.1 Лидерство и обязательства**

| |
|---|
| Высшее руководство должно демонстрировать лидерство и обязательства относительно СУИБ посредством:<br>a) гарантии того, что информационная политика безопасности и цели в сфере информационной безопасности установлены и согласуются со стратегическим руководством организации;<br>b) обеспечения интеграции требований СУИБ в процессы организации;<br>c) гарантии доступности ресурсов, необходимых для СУИБ;<br>d) информирования о важности эффективного управления информационной безопасностью и соответствия требованиям СУИБ;<br>e) гарантии того, что СУИБ достигает намеченных результатов;<br>f) направления и поддержки усилий сотрудников по обеспечению эффективности СУИБ;<br>g) продвижения непрерывного улучшения;<br>h) поддержки иных соответствующих функций руководства для демонстрации их лидерства в рамках установленной области их ответственности. |

Стандарты, относящиеся к системам управления, устанавливают общие и специальные требования. Специальные требования устанавливаются для процесса, в том числе требования по взаимодействию процессов.

Большинство специальных требований ИСО/МЭК 27001 содержится в настоящем приложении.

### А.5 Иллюстрирующий пример

Пример объясняет отношения между аспектами требований процессов (т. е. с точки зрения ИСО/МЭК 27001) и аспектами процесса согласно ИСО/МЭК 33002. Пример относится к процессу аудита. Этот процесс хорошо понимаем в терминах ожидаемых выходных результатов (т. е. в терминах потребностей в оценке соответствия), включая исчерпывающий набор требований, установленных в ИСО/МЭК 27001.

#### А.5.1 Требования к аудиту и процесс аудита

Каждый процесс, начиная с 5.2 по 5.27, поддержан с помощью раздела по прослеживаемости требований. Этот раздел предоставляет информацию о требованиях, которые поддерживаются выходными результатами процесса в настоящем стандарте. В большинстве случаев выходные результаты процесса поддержаны соответствующими требованиями из нескольких подразделов. Тем самым указывается, что требования для процесса, который реализован в пределах систем управления, в общем случае более широкие, чем заголовок соответствующего подраздела.

Отношения между аспектами процесса ЭМП (т. е. выходными результатами) и аспектами специальных требований, установленных в ИСО/МЭК 27001, приведены в таблице А.1.

Таблица А.1 — Процесс внутреннего аудита: аспекты ЭМП и специальные требования по ИСО/МЭК 27001

| Аспекты ЭМП | | Аспекты требований ИСО/МЭК 27001 | |
|---|---|---|---|
| Результаты процесса | Описание результатов процесса | Ссылка | Формулировка специальных требований |
| 1 | Определяется область и цели каждого аудита | 9.2 | a) соответствует ли СУИБ:<br>1) собственным требованиям организации к ее СУИБ;<br>2) требованиям настоящего стандарта |
| | | A.18.2.3 | Информационные системы должны регулярно анализироваться на соответствие политикам и стандартам информационной безопасности организации |

*Окончание таблицы А.1*

| Аспекты ЭМП | | Аспекты требований ИСО/МЭК 27001 | |
|---|---|---|---|
| Результаты процесса | Описание результатов процесса | Ссылка | Формулировка специальных требований |
| 2 | Получаются гарантии объективности и беспристрастности при проведении аудита и выборе аудиторов | 9.2 | Организации следует:<br>e) выбирать аудиторов и проводить аудиты так, чтобы гарантировать объективность и беспристрастность процесса аудита |
| 3 | Определяется соответствие выбранных продукции, услуг и процессов с требованиями, планами и соглашениями | 9.2 | Организация должна проводить внутренние аудиты через запланированные интервалы времени, чтобы получать соответствующую информацию |
| | | A.15.2.1 | Организации должны регулярно отслеживать, анализировать и проводить аудит предоставления услуги поставщиком |
| | | A.18.2.1 | Подход организации к управлению информационной безопасностью и его реализация (т. е. задачи управления, средства управления, политики, процессы и процедуры по обеспечению информационной безопасности) должны подвергаться независимому анализу через запланированные интервалы времени или в тех случаях, когда происходят существенные изменения |
| | | A.18.2.2 | Руководители в пределах своей области ответственности должны регулярно анализировать соответствие обработки информации и процедур политикам безопасности, стандартам и любым другим требованиям по безопасности |
| 4 | Формируются результаты аудита | 9.2 | Организации следует:<br>g) сохранять документированную информацию как подтверждение программы аудита и его результатов |

### А.6 Связь требований с результатами процесса

Связь подразделов и отдельных требований с соответствующими выходными результатами приведена в таблице А.2.

Таблица А.2 — Связь требований ИСО/МЭК 27001 с результатами процесса

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Понимание организации и ее среды<br>1 Организация должна определить внешние и внутренние проблемы, которые значимы с точки зрения ее целей и которые влияют на способность ее СУИБ достигать ожидаемых результатов | 04.1 | TOP.1 | Лидерство<br>1 Изучается и анализируется среда организации, включая ожидания ее заинтересованных сторон |
| Понимание потребностей и ожиданий заинтересованных сторон<br>1 Организация должна определить:<br>а) заинтересованные стороны, которые имеют существенное отношение к СУИБ и относящиеся к информационной безопасности | 04.2 | TOP.1 | Лидерство<br>1 Изучается и анализируется среда организации, включая ожидания ее заинтересованных сторон |
| Понимание потребностей и ожиданий заинтересованных сторон<br>2 Организация должна определить:<br>б) требования этих заинтересованных сторон | 04.2 | TOP.1 | Лидерство<br>1 Изучается и анализируется среда организации, включая ожидания ее заинтересованных сторон |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Определение области действия СУИБ<br>1 Организация должна определить границы и применимость СУИБ, чтобы установить область ее действия | 04.3 | TOP.1 | Лидерство<br>2 С учетом среды организации определяется область действий системы управления |
| Определение области действия СУИБ<br>2 Определяя эту область, организация должна принять во внимание:<br>a) внешние и внутренние проблемы, упомянутые в подразделе 4.1;<br>b) требования, упомянутые в подразделе 4.2;<br>c) взаимосвязи и зависимости между действиями, выполняемыми организацией, и теми, что выполняются другими организациями | 04.3 | TOP.1 | Лидерство<br>2 С учетом среды организации определяется область действий системы управления |
| Определение области действия СУИБ<br>3 Область действия должна быть оформлена в виде документируемой информации | 04.3 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| СУИБ<br>1 Организация должна установить, внедрить, поддерживать функционирование и непрерывно улучшать СУИБ в соответствии с требованиями настоящего стандарта | 04.4 | TOP.1 | Лидерство<br>4 Определяются система управления и эксплуатационная стратегия процесса |
| Лидерство и обязательства<br>1 Высшее руководство должно демонстрировать лидерство и обязательства относительно СУИБ посредством:<br>a) гарантии того, что информационная политика безопасности и цели в сфере информационной безопасности установлены и согласуются со стратегическим руководством организации;<br>b) обеспечения интеграции требований СУИБ в процессы организации;<br>c) гарантии доступности ресурсов, необходимых для СУИБ;<br>d) информирования о важности эффективного управления информационной безопасностью и соответствия требованиям СУИБ;<br>e) гарантии того, что СУИБ достигает намеченных результатов;<br>f) направления и поддержки усилий сотрудников по обеспечению эффективности СУИБ;<br>g) продвижения непрерывного улучшения;<br>h) поддержки иных соответствующих функций руководства для демонстрации их лидерства в рамках установленной области их ответственности | 05.1 | TOP.1 | Лидерство<br>5 Демонстрируются обязательство и лидерство согласно принятой системе управления |
| Лидерство и обязательства<br>2 Высшее руководство должно демонстрировать лидерство и обязательства относительно СУИБ посредством:<br>d) информирования о важности эффективного управления информационной безопасностью и соответствия требованиям СУИБ | 05.1 | COM.01 | Управление связью<br>6 Информационная продукция доводится до заинтересованных сторон |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Политика<br>1 Высшее руководство должно установить политику информационной безопасности, которая:<br>a) соответствует назначению организации;<br>b) включает цели (задачи) в области информационной безопасности, (см. подраздел 6.2) или служит основой для задания таких целей (задач);<br>c) включает обязательство соответствовать действующим требованиям, связанным с информационной безопасностью; и<br>d) включает обязательство непрерывного улучшения СУИБ | 05.2 | TOP.1 | Лидерство<br>3 Определяются политика системы управления и цели |
| Политика<br>2 Политика информационной безопасности должна:<br>e) быть оформлена как документируемая информация | 05.2 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Политика<br>3 Политика информационной безопасности должна:<br>f) быть доведена до сведения сотрудников в организации | 05.2 | COM.01 | Управление связью<br>6 Информационная продукция доводится до заинтересованных сторон |
| Политика<br>4 Политика информационной безопасности должна:<br>g) быть доступной в установленном порядке для заинтересованных сторон | 05.2 | COM.02 | Управление документацией<br>6 Документируемая информация становится доступной для заинтересованных сторон |
| Организационные функции, ответственность и полномочия<br>1 Высшее руководство должно гарантировать, что для функций, существенных с точки зрения информационной безопасности, ответственность и полномочия установлены [и доведены до сведения] | 05.3 | COM.09 | Функциональная реализация и управление<br>1 Распределяются необходимые функциональные обязанности, устанавливаются ответственность и полномочия |
| Организационные функции, ответственность и полномочия<br>2 Высшее руководство должно гарантировать, что для функций, существенных с точки зрения информационной безопасности, ответственность и полномочия [установлены и] доведены до сведения | 05.3 | COM.01 | Управление связью<br>6 Информационная продукция доводится до заинтересованных сторон |
| Организационные функции, ответственность и полномочия<br>3 Высшее руководство [должно установить] ответственность и полномочия для:<br>a) обеспечения соответствия СУИБ требованиям настоящего стандарта;<br>b) отчета о функционировании СУИБ высшему руководству | 05.3 | COM.08 | Эксплуатационное планирование<br>5 Определяются необходимые компетенции и функции для выполнения процесса |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Общее<br>1 Планируя СУИБ, организация должна принять во внимание проблемы, упомянутые в подразделе 4.1, и требования, установленные в подразделе 4.2 [а также определить риски и потенциальные возможности, которые необходимо принять во внимание, чтобы:<br>a) гарантировать, что СУИБ может достигать ожидаемых результатов;<br>b) предотвратить или уменьшить нежелательные эффекты;<br>c) обеспечивать непрерывное улучшение] | 06.1.1 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Общее<br>2 [Планируя СУИБ, организация должна принять во внимание проблемы, упомянутые в подразделе 4.1, и требования, установленные в подразделе 4.2, а также] определить риски и потенциальные возможности, которые необходимо принять во внимание, чтобы:<br>a) гарантировать, что СУИБ может достигать ожидаемых результатов;<br>b) предотвращать или уменьшать нежелательные эффекты;<br>c) обеспечивать непрерывное улучшение | 06.1.1 | COM.11 | Управление рисками и возможностями<br>1 Определяются риски |
| Общее<br>3 Организация должна планировать:<br>d) действия по выработке реакции на эти риски и реализации возможностей;<br>e) каким образом:<br>1) встраивать эти действия в процессы СУИБ и выполнять их,<br>2) оценивать результативность этих действий | 06.1.1 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Оценка рисков нарушения информационной безопасности<br>1 Организация должна определять [и применять] процесс оценки рисков нарушения информационной безопасности, который:<br>a) устанавливает и обеспечивает применение критериев оценки информационной безопасности, включающих в себя:<br>1) критерии приемлемости риска,<br>2) критерии для оценки рисков | 06.1.2 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Оценка рисков нарушения информационной безопасности<br>2 [Организация должна определять [и применять] процесс оценки рисков нарушения информационной безопасности, который:<br>a) устанавливает и обеспечивает применение критериев оценки информационной безопасности, включающие в себя]:<br>1) критерии приемлемости риска,<br>[2) критерии для оценки рисков] | 06.1.2 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Оценка рисков нарушения информационной безопасности<br>3 [Организация должна определять [и применять] процесс оценки рисков нарушения информационной безопасности, который:<br>a) устанавливает и обеспечивает применение критериев оценки информационной безопасности, включающих в себя:<br>1) критерии приемлемости риска,<br>2) критерии для оценки рисков | 06.1.2 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Оценка рисков нарушения информационной безопасности<br>4 Организация должна [определить и] применять процесс оценки рисков нарушения информационной безопасности, который:<br>a) устанавливает и обеспечивает применение критериев оценки информационной безопасности, включающие в себя:<br>1) критерии приемлемости риска,<br>2) критерии для оценки рисков | 06.1.2 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Оценка рисков нарушения информационной безопасности<br>5 b) гарантирует, что производимые оценки рисков нарушения информационной безопасности дают непротиворечивые, обоснованные и сопоставимые результаты | 06.1.2 | COM.09 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления |
| Оценка рисков нарушения информационной безопасности<br>6 c) обеспечивает выявление рисков нарушения информационной безопасности:<br>1) включает в себя процесс оценки рисков, направленный на идентификацию рисков, связанных с потерей конфиденциальности, целостности и возможности применения информации в рамках области действия СУИБ;<br>2) обеспечивает определение владельцев риска | 06.1.2 | COM.11 | Управление рисками и возможностями<br>1 Определяются риски |
| Оценка рисков нарушения информационной безопасности<br>7 d) обеспечивает анализ рисков нарушения информационной безопасности:<br>1) оценку потенциальных последствий в том случае, если бы риски, идентифицированные при выполнении требований 6.1.2 c 1), реализовались,<br>2) оценку реальной вероятности реализации рисков, идентифицированных при выполнении требований 6.1.2 c 1),<br>3) определение величины риска | 06.1.2 | COM.11 | Управление рисками и возможностями<br>2 Анализируются определенные риски |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Оценка рисков нарушения информационной безопасности<br>8 e) обеспечивает оценку рисков нарушения информационной безопасности:<br>1) сравнение результатов анализа рисков по критериям, установленным при выполнении требований 6.1.2 a),<br>2) расстановку рисков по приоритетам для последующей реакции на риски | 06.1.2 | COM.11 | Управление рисками и возможностями<br>2 Риски оцениваются по определенным критериям |
| Оценка рисков нарушения информационной безопасности<br>9 Организация должна сохранять данные процесса оценки рисков нарушения информационной безопасности как документируемую информацию | 06.1.2 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Реакция на риски нарушения информационной безопасности<br>1 Организация должна определять [и выполнять] процесс реакции на риски нарушения информационной безопасности с целью:<br>a) выбора соответствующих методов реакции на риски с учетом результатов оценки рисков;<br>b) определения любых средств управления, необходимых для реализации выбранных методов реакции на риски;<br>c) сравнения средств управления, определенных при выполнении требований 6.1.3 b), с приведенными в приложении А, чтобы удостовериться в том, что никакие из необходимых средств управления не были упущены из виду;<br>d) формирования Положения о применении, которое содержит:<br>- необходимые средства управления [см. 6.1.3 b) и c)],<br>- обоснование их применения,<br>- отметку о том, применяются ли эти средства управления в данный момент или нет, а также<br>- обоснование исключения любых средств, приведенных в приложении А;<br>e) разработки плана реакции на риски;<br>f) согласования плана с владельцами риска и подтверждения ими принятия остаточных рисков управления, приведенных в приложении | 06.1.3 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Реакция на риски нарушения информационной безопасности<br>2 Организация должна [определить и] выполнять процесс реакции на риски нарушения информационной безопасности с целью… | 06.1.3 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Реакция на риски нарушения информационной безопасности<br>3 e) разработки плана реакции на риски | 06.1.3 | COM.11 | Управление рисками и возможностями<br>4 Выбираются риски для соответствующей реакции по ним |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Реакция на риски нарушения информационной безопасности<br>4 f) согласования плана с владельцами риска и подтверждения ими принятия остаточных рисков | 06.1.3 | COM.02 | Управление документацией<br>5 Доводится по определенным критериям документируемая информация |
| Реакция на риски нарушения информационной безопасности<br>5 Организация должна сохранять данные процесса реакции на риски нарушения информационной безопасности как документируемую информацию | 06.1.3 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Цели в области информационной безопасности и планирование их достижения<br>1 Организация должна установить цели в области информационной безопасности для соответствующих функций и уровней | 06.2 | TOP.1 | Лидерство<br>3 Определяются политика системы управления и цели |
| Цели в области информационной безопасности и планирование их достижения<br>2 Цели в области информационной безопасности должны:<br>a) быть согласованными с политикой информационной безопасности;<br>b) быть измеримыми (если возможно);<br>c) учитывать действующие требования к информационной безопасности, а также результаты оценки и реакции на риски;<br>d) быть сообщены персоналу;<br>e) соответствующим образом обновляться | 06.2 | TOP.1 | Лидерство<br>3 Определяются политика системы управления и цели |
| Цели в области информационной безопасности и планирование их достижения<br>3 Цели в области информационной безопасности должны:<br>b) быть измеримыми (если возможно) | 06.2 | COM.10 | Оценка функционирования<br>1 Определяются потребности в контроле и оценках функционирования |
| Цели в области информационной безопасности и планирование их достижения<br>4 Цели в области информационной безопасности должны:<br>d) быть сообщены персоналу | 06.2 | COM.01 | Управление связью<br>6 Информационная продукция доводится до заинтересованных сторон |
| Цели в области информационной безопасности и планирование их достижения<br>5 Цели в области информационной безопасности должны:<br>e) соответствующим образом обновляться | 06.2 | COM.02 | Управление документацией<br>3 Становится известным статус содержания документируемой информации |
| Цели в области информационной безопасности и планирование их достижения<br>6 Организация должна сохранять данные по целям в области информационной безопасности как документируемую информацию | 06.2 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Цели в области информационной безопасности и планирование их достижения<br>7 При планировании способов достижения своих целей в области информационной безопасности организация должна определить:<br>f) что будет сделано | 06.2 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Цели в области информационной безопасности и планирование их достижения<br>8 При планировании способов достижения своих целей в области информационной безопасности организация должна определить:<br>g) какие ресурсы потребуются | 06.2 | COM.08 | Эксплуатационное планирование<br>6 Определяются требуемые ресурсы для выполнения процесса |
| Цели в области информационной безопасности и планирование их достижения<br>9 При планировании способов достижения своих целей в области информационной безопасности организация должна определить:<br>h) кто будет ответственным | 06.2 | COM.08 | Эксплуатационное планирование<br>5 Определяются необходимые компетенции и функции для выполнения процесса |
| Цели в области информационной безопасности и планирование их достижения<br>10 При планировании способов достижения своих целей в области информационной безопасности организация должна определить:<br>i) когда цели будут достигнуты | 06.2 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Цели в области информационной безопасности и планирование их достижения<br>11 При планировании способов достижения своих целей в области информационной безопасности организация должна определить:<br>j) как результаты будут оцениваться | 06.2 | COM.08 | Эксплуатационное планирование<br>7 Определяются методы для контроля эффективности и приемлемости процесса |
| Ресурсы<br>1 Организация должна определить [и обеспечить] ресурсы, необходимые для разработки, внедрения, поддержания функционирования и непрерывного улучшения СУИБ | 07.1 | COM.08 | Эксплуатационное планирование<br>6 Определяются требуемые ресурсы для выполнения процесса |
| Ресурсы<br>2 Организация должна [определить и] обеспечить ресурсы, необходимые для разработки, внедрения, поддержания функционирования и непрерывного улучшения СУИБ | 07.1 | COM.09 | Эксплуатационное планирование<br>2 Распределяются и используются требуемые ресурсы |
| Компетентность<br>1 Организация должна:<br>a) определять необходимую компетентность персонала, который выполняет работу под контролем организации и который влияет на информационную безопасность | 07.2 | COM.08<br><br><br><br><br>COM.03 | Эксплуатационное планирование<br>5 Определяются необходимые компетенции и функции для выполнения процесса.<br>Управление человеческими ресурсами<br>1 Определяются компетенции, требуемые организации для производства продукции и услуг |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Компетентность<br>2 Организация должна:<br>b) гарантировать, что этот персонал компетентен в силу соответствующего образования, подготовки и/или опыта | 07.2 | COM.03 | Управление человеческими ресурсами<br>3 Каждый работник проявляет понимание своих функций и действий для достижения целей организации в обеспечении производства продукции и услуг |
| Компетентность<br>3 Организация должна:<br>c) там, где это возможно, предпринимать меры для обеспечения необходимой компетентности [и оценивать результативность предпринятых мер] | 07.2 | COM.03 | Управление человеческими ресурсами<br>2 Определенный уровень компетенции достигается путем обучения или найма работников |
| Компетентность<br>4 Организация должна:<br>c) [там, где это возможно, предпринимать меры для обеспечения необходимой компетентности и] оценивать результативность предпринятых мер | 07.2 | COM.09 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления |
| Компетентность<br>5 Организация должна:<br>d) сохранять соответствующую документируемую информацию как доказательства компетентности | 07.2 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Осведомленность<br>1 Персонал, выполняющий работу под контролем организации, должен знать:<br>a) политику в области информационной безопасности;<br>b) их вклад в результативность СУИБ, включая выгоды от улучшения деятельности по обеспечению информационной безопасности;<br>c) последствия несоответствий требованиям СУИБ | 07.3 | COM.03 | Управление человеческими ресурсами<br>3 Каждый работник проявляет понимание своих функций и действий для достижения целей организации в обеспечении производства продукции и услуг |
| Связь<br>1 Организация должна определить потребность во внутренних и внешних коммуникациях, существенных для функционирования СУИБ, включая:<br>a) содержание информации для обмена | 07.4 | COM.01 | Управление связью<br>1 Содержание информации определяется в терминах требований и потребностей связи |
| Связь<br>2 Организация должна определить потребность во внутренних и внешних коммуникациях, существенных для функционирования СУИБ, включая:<br>b) когда обмениваться информацией | 07.4 | COM.01 | Управление связью<br>4 Определяются события, требующие коммуникационных действий |
| Связь<br>3 Организация должна определить потребность во внутренних и внешних коммуникациях, существенных для функционирования СУИБ, включая:<br>c) с кем обмениваться информацией | 07.4 | COM.01 | Управление связью<br>2 Определяются стороны для связи |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Связь<br>4 Организация должна определить потребность во внутренних и внешних коммуникациях, существенных для функционирования СУИБ, включая:<br>d) кто должен обмениваться информацией | 07.4 | COM.01 | Управление связью<br>3 Определяется сторона, ответственная за связь |
| Связь<br>5 Организация должна определить потребность во внутренних и внешних коммуникациях, существенных для функционирования СУИБ, включая:<br>e) процессы, посредством которых должна осуществляться связь | 07.4 | COM.01 | Управление связью<br>5 Определяется канал связи |
| Общее<br>1 СУИБ организации должна включать:<br>a) документируемую информацию, требуемую настоящим стандартом;<br>b) документируемую информацию, признанную организацией необходимой для обеспечения результативности СУИБ | 07.5.1 | TOP.1 | Лидерство<br>4 Определяется система управления и эксплуатационная стратегия процесса |
| Создание и обновление<br>1 Создавая и обновляя документируемую информацию, организация должна обеспечить соответствующие:<br>a) идентификацию и выходные данные (например, название, дата, автор или ссылочный номер) | 07.5.2 | COM.02 | Управление документацией<br>2 Определяются формы представления документируемой информации |
| Создание и обновление<br>2 Создавая и обновляя документированную информацию организация должна обеспечить соответствующие:<br>b) формат (например, язык, версия программного обеспечения, графики) и носитель (например, бумага, электронный вид) | 07.5.2 | COM.02 | Управление документацией<br>2 Определяются формы представления документируемой информации |
| Создание и обновление<br>3 Создавая и обновляя документированную информацию организация должна обеспечить соответствующие:<br>c) анализ [и утверждение] в целях сохранения пригодности и соответствия | 07.5.2 | COM.02 | Управление документацией<br>2 Определяются формы представления документируемой информации |
| Создание и обновление<br>3 Создавая и обновляя документированную информацию организация должна обеспечить соответствующие:<br>c) [анализ и] утверждение в целях сохранения пригодности и соответствия | 07.5.2 | COM.02 | Управление документацией<br>5 Доводится по определенным критериям документируемая информация |
| Управление документируемой информацией<br>1 Документируемой информацией, требуемой СУИБ и настоящим стандартом, необходимо управлять, чтобы гарантировать, что она:<br>a) доступна и пригодна для применения там, где и когда она необходима; | 07.5.3 | TOP.1 | Лидерство<br>4 Определяется система управления и эксплуатационная стратегия процесса |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| b) надлежащим образом защищена (например, от потери конфиденциальности, неправильного использования или потери целостности). Для управления документируемой информацией организация должна осуществлять следующие действия, насколько это применимо:<br>c) рассылать, обеспечивать доступ, выдачу и применение,<br>d) хранить и сохранять в надлежащем состоянии, включая сохранение читаемости,<br>e) контролировать изменения (например, контроль версий),<br>f) устанавливать срок хранения и методы уничтожения | | | |
| Управление документируемой информацией<br>2 a) доступна и пригодна для применения там, где и когда она необходима | 07.5.3 | COM.02 | Управление документацией<br>6 Документируемая информация становится доступной для заинтересованных сторон |
| Управление документируемой информацией<br>3 b) надлежащим образом защищена (например, от потери конфиденциальности, неправильного использования или потери целостности) | 07.5.3 | COM.02 | Управление документацией<br>4 Документируемая информация является обновляемой, полной и достоверной |
| Управление документируемой информацией<br>4 c) рассылать, обеспечивать доступ, выдачу и применение | 07.5.3 | COM.02 | Управление документацией<br>6 Документируемая информация становится доступной для заинтересованных сторон |
| Управление документируемой информацией<br>5 d) хранить и сохранять в надлежащем состоянии, включая сохранение читаемости | 07.5.3 | COM.02 | Управление документацией<br>7 Документируемая информация архивируется или уничтожается, как это требуется |
| Управление документируемой информацией<br>6 e) контролировать изменения (например, контроль версий) | 07.5.3 | COM.02 | Управление документацией<br>3 Становится известным статус содержания документируемой информации |
| Управление документируемой информацией<br>7 f) устанавливать срок хранения и методы уничтожения | 07.5.3 | COM.02 | Управление документацией<br>7 Документируемая информация архивируется или уничтожается |
| Управление документируемой информацией<br>8 Документируемая информация внешнего происхождения, признанная организацией необходимой для планирования и функционирования СУИБ, должна быть идентифицирована соответствующим образом и управляться | 07.5.3 | COM.02 | Управление документацией<br>2 Определяются формы представления документируемой информации |
| Эксплуатационное планирование и контроль<br>1 Организация должна планировать, осуществлять и управлять процессами, необходимыми для обеспечения соответствия требованиям, и выполнять действия, определенные в 6.1 | 08.1 | TOP.1 | Лидерство<br>4 Определяется система управления и эксплуатационная стратегия процесса |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Эксплуатационное планирование и контроль<br>2 Организация должна также выполнять запланированные действия для достижения целей, определенных в.6.2 | 08.1 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Эксплуатационное планирование и контроль<br>3 Организация должна сохранять документированную информацию в объеме, необходимом для обеспечения уверенности, что процессы были выполнены, как было запланировано | 08.1 | COM.02 | Управление документацией<br>7 Документируемая информация архивируется или уничтожается, как то требуется |
| Эксплуатационное планирование и контроль<br>4 Организация должна [управлять запланированными изменениями и] анализировать последствия непреднамеренных изменений, принимая, по мере необходимости, меры для снижения любых отрицательных воздействий | 08.1 | COM.09 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления |
| Эксплуатационное планирование и контроль<br>5 Организация должна управлять запланированными изменениями [и анализировать] последствия непреднамеренных изменений, принимая, по мере необходимости, меры для снижения любых отрицательных воздействий | 08.1 | COM.09<br><br><br><br><br>COM.09 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления<br>Функциональная реализация и управление<br>5 При недостижении целей исправляются отклонения в планируемых действиях |
| Эксплуатационное планирование и контроль<br>6 Организация должна гарантировать, что переданные для выполнения на сторону процессы определены и управляются | 08.1 | TOP.1 | Лидерство<br>4 Определяется система управления и эксплуатационная стратегия процесса |
| Оценка рисков нарушения информационной безопасности<br>1 Организация должна выполнять оценку рисков нарушения информационной безопасности с учетом критериев, установленных в 6.1.2, а) [через запланированные интервалы времени или когда предложены или произошли существенные изменения] | 08.2 | COM.11 | Управление рисками и возможностями<br>1 Определяются риски |
| Оценка рисков нарушения информационной безопасности<br>2 [Организация должна выполнять оценку рисков нарушения информационной безопасности с учетом критериев, установленных в 6.1.2, а)] через запланированные интервалы времени или когда предложены или произошли существенные изменения | 08.2 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Оценка рисков нарушения информационной безопасности<br>3 Организация должна сохранять результаты оценки рисков нарушения информационной безопасности как документируемую информацию | 08.2 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Реакция на риск нарушения информационной безопасности<br>1 Организация должна осуществлять план реакции на риски нарушения информационной безопасности | 08.3 | COM.11 | Управление рисками и возможностями<br>5 Осуществляется реакция на выбранные риски |
| Реакция на риск нарушения информационной безопасности<br>2 Организация должна сохранять результаты реакции на риски нарушения информационной безопасности как документированную информацию | 08.3 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Мониторинг, измерение, анализ и оценка<br>1 Организация должна оценивать функционирование и результативность СУИБ | 09.1 | COM.10 | Оценка функционирования<br>5 Анализируются собираемые данные о функционировании |
| Мониторинг, измерение, анализ и оценка<br>2 Организация должна определить:<br>a) что должно быть объектом мониторинга и измерений, включая процессы и средства управления информационной безопасностью | 09.1 | COM.10 | Оценка функционирования<br>1 Определяются потребности в контроле и оценках функционирования |
| Мониторинг, измерение, анализ и оценка<br>3 b) методы мониторинга, измерения, анализа и оценки, насколько это применимо, чтобы гарантировать пригодные результаты | 09.1 | COM.10 | Оценка функционирования<br>3 Определяются методы измерений, поддерживающие показатели оценки функционирования |
| Мониторинг, измерение, анализ и оценка<br>4 c) когда должен выполняться мониторинг и измерения | 09.1 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Мониторинг, измерение, анализ и оценка<br>5 d) кто должен осуществлять мониторинг и измерения | 09.1 | COM.08 | Эксплуатационное планирование<br>5 Определяются необходимые компетенции и функции для выполнения процесса |
| Мониторинг, измерение, анализ и оценка<br>6 e) когда результаты мониторинга и измерений должны анализироваться и оцениваться | 09.1 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Мониторинг, измерение, анализ и оценка<br>7 f) кто должен анализировать и оценивать эти результаты | 09.1 | COM.08 | Эксплуатационное планирование<br>5 Определяются необходимые компетенции и функции для выполнения процесса |
| Мониторинг, измерение, анализ и оценка<br>8 Организация должна сохранять результаты мониторинга и измерений как документированную информацию | 09.1 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Внутренний аудит<br>1 Организация должна проводить внутренние аудиты [через запланированные интервалы времени], чтобы получать информацию о том, что СУИБ: | 09.2 | COM.05 | Внутренний аудит<br>3 Определяется соответствие выбранных услуг, продукции и процессов требованиям, планам и соглашениям |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Внутренний аудит<br>2 [Организация должна проводить внутренние аудиты] через запланированные интервалы времени [чтобы получать информацию о том, что СУИБ:] | 09.2 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Внутренний аудит<br>3 a) соответствует:<br>1) собственным требованиям организации к ее СУИБ,<br>2) требованиям настоящего стандарта | 09.2 | COM.05 | Внутренний аудит<br>1 Определяется область проведения и цель каждого аудита |
| Внутренний аудит<br>4 b) эффективно реализована [и поддерживается] | 09.2 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Внутренний аудит<br>5 b) [эффективно реализована] и поддерживается | 09.2 | COM.09 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления |
| Внутренний аудит<br>6 Организация должна:<br>c) планировать, устанавливать, [реализовывать и поддерживать] программы аудитов, включая периодичность их проведения, методы, ответственность, требования к планированию и отчетности | 09.2 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Внутренний аудит<br>7 Организация должна:<br>c) [планировать, устанавливать], реализовывать и поддерживать программы аудитов, включая периодичность их проведения, методы, ответственность, требования к планированию и отчетности | 09.2 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Внутренний аудит<br>8 Организация должна: в программе аудитов учитывать значимость проверяемых процессов и результаты предыдущих аудитов | 09.2 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Внутренний аудит<br>9 Организация должна:<br>d) определить критерии и область аудита для каждой проверки | 09.2 | COM.05 | Внутренний аудит<br>1 Определяется область проведения и цель каждого аудита |
| Внутренний аудит<br>10 Организация должна:<br>e) выбирать аудиторов и проводить аудиты так, чтобы гарантировать объективность и беспристрастность процесса аудита | 09.2 | COM.05 | Внутренний аудит<br>2 Обеспечивается объективность и беспристрастность проведения аудитов и выбора аудиторов |
| Внутренний аудит<br>11 Организация должна:<br>f) гарантировать, что результаты аудитов переданы соответствующим руководителям | 09.2 | COM.01 | Управление связью<br>6 Информационная продукция доводится до заинтересованных сторон |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Внутренний аудит<br>12 Организация должна:<br>g) сохранять [документируемую] информацию как подтверждение программы аудита и его результатов | 09.2 | COM.05 | Внутренний аудит<br>3 Соответствие требованиям выбранных услуг, продукции и процессов |
| Внутренний аудит<br>13 [Организация должна:<br>g) сохранять] документированную информацию как подтверждение [программы аудита и его результатов] | 09.2 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Анализ управления<br>1 Высшее руководство должно анализировать СУИБ организации через запланированные интервалы времени, чтобы гарантировать ее постоянную пригодность, соответствие и результативность | 09.3 | COM.06 | Анализ управления<br>2 В терминах установленных целей оцениваются статус и выполнение действий процесса |
| Анализ управления<br>2 [Высшее руководство должно анализировать СУИБ организации] через запланированные интервалы времени [чтобы гарантировать ее постоянную пригодность, соответствие и результативность] | 09.3 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Анализ управления<br>3 При анализе управления необходимо учитывать следующее:<br>a) статус мероприятий, предусмотренных предыдущим анализом;<br>b) изменения в состоянии внешних и внутренних проблем, которые существенны для СУИБ;<br>c) информацию о функционировании СУИБ, включая тенденции в: 1) несоответствиях и корректирующих действиях, 2) результатах мониторинга и измерений, 3) результатах аудитов и 4) достижении целей в области информационной безопасности;<br>d) обратную связь от заинтересованных сторон;<br>e) результаты оценки рисков и статус выполнения плана реакции на риски;<br>f) возможности для постоянного улучшения | 09.3 | COM.06 | Анализ управления<br>1 Устанавливаются цели анализа |
| Анализ управления<br>4 Результаты анализа должны включать решения, связанные с возможностями непрерывного улучшения и любыми потребностями в изменениях СУИБ | 09.3 | COM.04<br><br><br>COM.06 | Улучшения<br>1 Определяются возможности для улучшения<br>Анализ управления<br>3 Определяются риски, проблемы и возможности для улучшения |
| Анализ управления<br>5 Организация должна сохранять документированную информацию как подтверждение результатов анализа системы управления | 09.3 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Несоответствия и корректирующие действия<br>1 При выявлении несоответствия… | 10.1 | COM.07 | Управление несоответствиями<br>1 Определяются несоответствия |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Несоответствия и корректирующие действия<br>2 [При выявлении несоответствия], организация должна:<br>a) реагировать на несоответствие и, насколько применимо:<br>1) принять меры для управления им и его исправления | 10.1 | COM.07 | Управление несоответствиями<br>2 Несоответствия разрешаются и закрываются |
| Несоответствия и корректирующие действия<br>3 [При выявлении несоответствия], организация должна:<br>b) оценивать потребность в действиях по устранению причины несоответствия с тем, чтобы оно не повторялось или не происходило в другом месте, [посредством:<br>1) анализа несоответствия,<br>2) определения причин несоответствий,<br>3) выявления, есть ли подобные несоответствия, или могут ли они потенциально произойти] | 10.1 | COM.07 | Управление несоответствиями<br>4 Оценивается потребность в действиях по устранению несоответствий |
| Несоответствия и корректирующие действия<br>4 [При выявлении несоответствия, организация должна:<br>b) оценивать потребность в действиях по устранению причины несоответствия с тем, чтобы оно не повторялось или не происходило в другом месте, посредством:<br>1) анализа несоответствия],<br>2) определения причин несоответствий,<br>3) выявления, есть ли подобные несоответствия, или могут ли они потенциально произойти | 10.1 | COM.07 | Управление несоответствиями<br>3 Определяются случаи выбранных несоответствий |
| Несоответствия и корректирующие действия<br>5 [При выявлении несоответствия] организация должна:<br>c) осуществлять любое необходимое действие | 10.1 | COM.07 | Управление несоответствиями<br>5 Реализуются предложения по выбранным действиям |
| Несоответствия и корректирующие действия<br>6 [При выявлении несоответствия] организация должна:<br>d) анализировать результативность всех предпринятых корректирующих действий | 10.1 | COM.07 | Управление несоответствиями<br>6 Подтверждается эффективность изменений для устранения несоответствий |
| Несоответствия и корректирующие действия<br>7 [При выявлении несоответствия] организация должна:<br>e) вносить изменения в СУИБ, если необходимо | 10.1 | COM.07 | Управление несоответствиями<br>5 Реализуются предложения по выбранным действиям |
| Несоответствия и корректирующие действия<br>8 Корректирующие действия должны соответствовать последствиям выявленных несоответствий | 10.1 | COM.07 | Управление несоответствиями<br>4 Оценивается потребность в действиях по устранению несоответствий |
| Несоответствия и корректирующие действия<br>9 Организация должна сохранять документированную информацию как свидетельство:<br>f) характера несоответствий и любых последующих предпринятых действий;<br>g) результатов любого корректирующего действия | 10.1 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Непрерывное улучшение<br>1 Организация должна непрерывно улучшать пригодность, соответствие и результативность СУИБ | 10.2 | TOP.1 | Лидерство<br>4 Определяется система управления и эксплуатационная стратегия процесса |
| Политики информационной безопасности<br>1 Должен быть разработан [одобрен руководством, опубликован и доведен до персонала и соответствующих внешних сторон комплекс политик информационной безопасности] | A.05.1.1 | TOP.1 | Лидерство<br>3 Определяются политика системы управления и цели |
| Политики информационной безопасности<br>2 Должен быть [разработан], одобрен руководством [опубликован и доведен до персонала и соответствующих внешних сторон комплекс политик информационной безопасности] | A.05.1.1 | COM.02 | Управление документацией<br>5 Доводится по определенным критериям документируемая информация |
| Политики информационной безопасности<br>3 Должен быть [разработан, одобрен руководством] опубликован [и доведен до персонала и соответствующих внешних сторон комплекс политик информационной безопасности] | A.05.1.1 | COM.02 | Управление документацией<br>6 Документируемая информация становится доступной для заинтересованных сторон |
| Политики информационной безопасности<br>4 Должен быть [разработан, одобрен руководством, опубликован и] доведен до персонала и соответствующих внешних сторон комплекс политик информационной безопасности | A.05.1.1 | COM.01 | Управление связью<br>6 Информационная продукция доводится до заинтересованных сторон |
| Анализ политик информационной безопасности<br>1 Политики информационной безопасности для гарантии их постоянной пригодности, соответствия и результативности должны анализироваться [через запланированные интервалы времени] или в случае существенных изменений | A.05.1.2 | COM.09 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления |
| Анализ политик информационной безопасности<br>2 Политики информационной безопасности для гарантии их постоянной пригодности, соответствия и результативности [должны анализироваться] через запланированные интервалы времени или в случае существенных изменений | A.05.1.2 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Должностные функции и ответственность, связанные с информационной безопасностью<br>1 Должны быть определены [и распределены] все обязанности, связанные с информационной безопасностью | A.06.1.1 | COM.08 | Эксплуатационное планирование<br>5 Определяются необходимые компетенции и функции для выполнения процесса |
| Должностные функции и ответственность, связанные с информационной безопасностью<br>2 Должны быть [определены] и распределены все обязанности, связанные с информационной безопасностью | A.06.1.1 | COM.09 | Функциональная реализация и управление<br>1 Распределяются необходимые функциональные обязанности, ответственность и полномочия |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Разделение обязанностей<br>1 Вступающие в противоречие друг с другом обязанности и области ответственности должны быть разделены для снижения возможности несанкционированного или ненамеренного изменения, или неправильного применения активов организации | A.06.1.2 | COM.08 | Эксплуатационное планирование<br>5 Определяются необходимые компетенции и функции для выполнения процесса |
| Контакты с полномочными органами<br>1 Должны поддерживаться соответствующие контакты с полномочными органами | A.06.1.3 | COM.01 | Управление связью<br>2 Определяются стороны для связи |
| Контакты с профессиональными сообществами<br>1 Должны поддерживаться соответствующие контакты с профессиональными сообществами или иными форумами специалистов по информационной безопасности и профессиональными ассоциациями | A.06.1.4 | COM.01 | Управление связью<br>2 Определяются стороны для связи |
| Информационная безопасность в управлении проектами<br>1 Информационная безопасность должна быть отражена в управлении проектами независимо от типа проекта | A.06.1.5 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Политика в отношении мобильных устройств<br>1 [Должны быть адаптированы] политика и меры по обеспечению безопасности для управления рисками, связанными с использованием мобильных устройств | A.06.2.1 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Политика в отношении мобильных устройств<br>2 Должны быть адаптированы политика [и поддерживающие меры] по обеспечению безопасности для управления рисками, связанными с использованием мобильных устройств | A.06.2.1 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Удаленная работа<br>1 Должны быть приняты политика [и поддерживающие меры] обеспечения безопасности для защиты информации, к которой осуществляется доступ на удаленных рабочих местах, и которая там обрабатывается или сохраняется | A.06.2.2 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Удаленная работа<br>2 [Должны быть приняты политика и] поддерживающие меры [обеспечения безопасности для защиты информации, к которой осуществляется доступ на удаленных рабочих местах, и которая там обрабатывается или сохраняется] | A.06.2.2 | COM.08 | Эксплуатационное планирование<br>3 Определяется множество действий, преобразующих входы в выходные результаты |
| Удаленная работа<br>3 Должны быть приняты [политика и поддерживающие меры обеспечения безопасности] для защиты информации, к которой осуществляется доступ на удаленных рабочих местах, и которая там обрабатывается или сохраняется | A.06.2.2 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Предварительная проверка<br>1 Проверка при приеме на работу, осуществляемая для всех кандидатов, должна проводиться в рамках соответствующих законодательных актов, регламентов и этических норм, а также должна быть соразмерна деловым требованиям, категории информации по классификации, к которой предполагается доступ, и предполагаемым рискам | A.07.1.1 | ORG.3 | Управление персоналом в период занятости<br>2 Предполагаемый персонал оценивается в соответствии с соответствующими законами, инструкциями и этикой согласно деловым требованиям и сформированным рискам |
| Условия трудового соглашения<br>1 Трудовые соглашения с сотрудниками или привлекаемыми по контракту должны устанавливать ответственность их и организации в части информационной безопасности | A.07.1.2 | ORG.3<br><br><br><br><br>ORG.3 | Управление персоналом в период занятости<br>3 Предполагаемый персонал соглашается с условиями и сроками их занятости по контракту<br>Управление персоналом в период занятости<br>1 Определяются функции и ответственность работников, нанимателей и исполнителей от других сторон |
| Ответственность руководства<br>1 Руководство должно требовать от всех сотрудников и работающих по контракту соблюдения требований по информационной безопасности в соответствии с установленными политиками и процедурами организации | A.07.2.1 | ORG.3 | Управление персоналом в период занятости<br>4 Для работников реализуются условия и сроки контракта |
| Осведомленность, образование и обучение в сфере информационной безопасности<br>1 Все сотрудники организации и, там, где это существенно, работающие по контракту должны быть соответствующим образом информированы и обучены, а также регулярно извещаться об изменениях в политиках и процедурах организации, в той мере, насколько это важно для исполнения их служебных обязанностей | A.07.2.2 | COM.03 | Управление человеческими ресурсами<br>3 Каждый работник проявляет понимание своих функций и действий для достижения целей организации в обеспечении производства продукции и услуг |
| Дисциплинарный процесс<br>1 Должен быть разработан [и доведен до сведения персонала] процесс для принятия мер к тем сотрудникам, которые допустили нарушение требований информационной безопасности | A.07.2.3 | ORG.3 | Управление персоналом в период занятости<br>6 Дисциплинарные меры применяются к работникам, которые нарушили согласованные условия контракта |
| Дисциплинарный процесс<br>2 Должен быть [разработан] и доведен до сведения персонала процесс для принятия мер к тем сотрудникам, которые допустили нарушение требований информационной безопасности | A.07.2.3 | COM.01 | Управление связью<br>6 Информационная продукция доводится до заинтересованных сторон |
| Освобождение от обязанностей или их изменение<br>1 Должны быть определены [доведены до сведения сотрудника или работающего по контракту] его область ответственности и обеспечено выполнение его обязанностей в отношении информационной безопасности, остающихся в силе после прекращения или изменения трудовых отношений | A.07.3.1 | ORG.3 | Управление персоналом в период занятости<br>7 Определяются и подписываются положения об ответственности за выполнение соглашения или изменениях |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Освобождение от обязанностей или их изменение<br>2 Должны быть [определены] доведены до сведения сотрудника или работающего по контракту его область ответственности и обеспечено выполнение его обязанностей в отношении информационной безопасности, остающихся в силе после прекращения или изменения трудовых отношений | A.07.3.1 | COM.01 | Управление связью<br>6 Информационная продукция доводится до заинтересованных сторон |
| Инвентаризация активов<br>1 Информация, другие активы, связанные с информацией и устройствами обработки информации, должны быть выявлены [и составлен реестр этих активов, который должен поддерживаться в актуальном состоянии] | A.08.1.1 | ORG.1 | Управление активами<br>1 Определяются объекты, подлежащие управлению активами |
| Инвентаризация активов<br>2 [Информация, другие активы, связанные с информацией и устройствами обработки информации, должны быть выявлены и] составлен реестр этих активов, [который должен поддерживаться в актуальном состоянии] | A.08.1.1 | ORG.1 | Управление активами<br>3 Активы инвентаризуются |
| Инвентаризация активов<br>3 [Информация, другие активы, связанные с информацией и устройствами обработки информации, должны быть выявлены и составлен реестр этих активов], который должен поддерживаться в актуальном состоянии | A.08.1.1 | ORG.1 | Управление активами<br>5 В рамках управления контролируются изменения в активах |
| Владение активами<br>1 У активов, включенных в реестр, должны быть владельцы | A.08.1.2 | COM.08 | Эксплуатационное планирование<br>5 Определяются необходимые компетенции и функции для выполнения процесса |
| Надлежащее использование активов<br>1 Правила для надлежащего использования информации и активов, связанных с информацией и устройствами обработки информации, должны быть определены [документированы и внедрены] | A.08.1.3 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Надлежащее использование активов<br>1 Правила для надлежащего использования информации и активов, связанных с информацией и устройствами обработки информации, должны быть [определены], документированы и [внедрены] | A.08.1.3 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Надлежащее использование активов<br>1 Правила для надлежащего использования информации и активов, связанных с информацией и устройствами обработки информации, должны быть [определены, документированы и внедрены] | A.08.1.3 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Возврат активов<br>1 Все сотрудники и внешние пользователи должны вернуть все активы организации в ее распоряжение по окончании действия трудовых договоров, контрактов и соглашений | A.08.1.4 | ORG.3 | Управление персоналом в период занятости<br>8 Работники возвращают все активы организации в ее владение после завершения периода занятости |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Классификация информации<br>1 Все сотрудники и внешние пользователи должны вернуть все активы организации в ее распоряжение по окончании действия трудовых договоров, контрактов и соглашений | A.08.2.1 | ORG.1 | Управление активами<br>2 Объекты, отнесенные к активам, классифицируются |
| Маркировка информации<br>1 Должен быть разработан [и внедрен] соответствующий набор процедур для маркировки информации в соответствии со схемой классификации информации, принятой в организации | A.08.2.2 | COM.08 | Эксплуатационное планирование<br>3 Определяется множество действий, преобразующих входы в выходные результаты |
| Маркировка информации<br>1 Должен быть [разработан и] внедрен соответствующий набор процедур для маркировки информации в соответствии со схемой классификации информации, принятой в организации | A.08.2.2 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Обращение с активами<br>1 Должны быть разработаны [и внедрены] процедуры обращения с активами в соответствии со схемой классификации информации, принятой в организации | A.08.2.3 | COM.08 | Эксплуатационное планирование<br>3 Определяется множество действий, преобразующих входы в выходные результаты |
| Обращение с активами<br>2 Должны быть [разработаны] и внедрены процедуры обращения с активами в соответствии со схемой классификации информации, принятой в организации | A.08.2.3 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Управление съемными носителями<br>1 Должны быть [внедрены] процедуры для управления съемными носителями в соответствии со схемой классификации, принятой в организации | A.08.3.1 | COM.08 | Эксплуатационное планирование<br>3 Определяется множество действий, преобразующих входы в выходные результаты |
| Управление съемными носителями<br>2 [Должны быть] внедрены [процедуры для управления съемными носителями в соответствии со схемой классификации, принятой в организации] | A.08.3.1 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Утилизация носителей информации<br>1 Носители [если в них больше нет необходимости, должны быть утилизированы] надежным способом в соответствии с установленными процедурами | A.08.3.2 | COM.08 | Эксплуатационное планирование<br>3 Определяется множество действий, преобразующих входы в выходные результаты |
| Утилизация носителей информации<br>2 Носители, если в них больше нет необходимости, должны быть утилизированы надежным способом [в соответствии с установленными процедурами] | A.08.3.2 | ORG.1 | Управление активами<br>5 В рамках управления контролируются изменения в активах |
| Физическое перемещение носителей информации<br>1 Носители информации во время транспортировки должны быть защищены от несанкционированного доступа, нецелевого использования или повреждения | A.08.3.3 | ORG.1 | Управление активами<br>5 В рамках управления контролируются изменения в активах |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Политика контроля доступа<br>1 Политика контроля доступа должна быть сформулирована [документирована и анализироваться с точки зрения требований бизнеса и информационной безопасности] | A.09.1.1 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Политика контроля доступа<br>2 Политика контроля доступа должна быть [сформулирована ], документирована [и анализироваться с точки зрения требований бизнеса и информационной безопасности] | A.09.1.1 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Политика контроля доступа<br>3 Политика контроля доступа должна быть [сформулирована, документирована и] анализироваться с точки зрения требований бизнеса и информационной безопасности | A.09.1.1 | COM.09 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления |
| Доступ к сетям и сетевым службам<br>1 Пользователи должны получать доступ только к тем сетям и сетевым службам, для которых у них есть авторизация | A.09.1.2 | ORG.4 | Инфраструктура и рабочая среда<br>6 Контролируется доступ к информационным ресурсам |
| Регистрация и отмена регистрации пользователя<br>1 Должен быть [внедрен] формализованный процесс регистрации и отмены регистрации пользователей, обеспечивающий возможность назначения прав доступа | A.09.2.1 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Регистрация и отмена регистрации пользователя<br>1 Должен быть внедрен формализованный процесс регистрации и отмены регистрации пользователей, обеспечивающий возможность назначения прав доступа | A.09.2.1 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Предоставление доступа пользователю<br>1 Должен быть внедрен формализованный процесс предоставления доступа пользователям для назначения или отмены прав всем типам пользователей ко всем системам и услугам | A.09.2.2 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Управление привилегированными правами доступа<br>1 Назначение и использование привилегированных прав доступа должно быть ограниченным и контролируемым | A.09.2.3 | ORG.4 | Инфраструктура и рабочая среда<br>6 Контролируется доступ к информационным ресурсам |
| Управление секретной аутентификационной информацией пользователей<br>1 Присваивание секретной информации аутентификации [должно быть контролируемым через] формализованный процесс управления | A.09.2.4 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Управление секретной аутентификационной информацией пользователей<br>1 [Присваивание секретной информации аутентификации] должно быть контролируемым [через формализованный процесс управления] | A.09.2.4 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Пересмотр прав доступа пользователей<br>1 Владельцы активов должны пересматривать права доступа пользователей [через регулярные промежутки времени] | A.09.2.5 | ORG.4 | Инфраструктура и рабочая среда<br>6 Контролируется доступ к информационным ресурсам |
| Пересмотр прав доступа пользователей<br>1 Владельцы активов [должны пересматривать права доступа пользователей] через регулярные промежутки времени | A.09.2.5 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Отмена или изменение прав доступа<br>1 Права доступа к информации и устройствам обработки информации всех сотрудников и внешних пользователей должны быть отменены после завершения трудовых отношений, контракта или соглашения | A.09.2.6 | ORG.3 | Управление персоналом в период занятости<br>9 Доступ работников к информационным ресурсам прекращается по завершении контракта |
| Использование секретной информации аутентификации<br>1 Пользователи обязаны следовать правилам организации при использовании секретной аутентификационной информации | A.09.3.1 | ORG.3 | Управление персоналом в период занятости<br>3 Предполагаемый персонал соглашается с условиями и сроками их занятости по контракту |
| Ограничение доступа к информации<br>1 Доступ к информации и функциям прикладных систем должен быть ограничен в соответствии с политикой контроля доступа | A.09.4.1 | ORG.4 | Инфраструктура и рабочая среда<br>2 Определяются права доступа к информационным ресурсам |
| Безопасные процедуры входа в систему<br>1 Там, где это требуется политикой контроля доступа, доступ к системам и приложениям должен осуществляться в соответствии с безопасной процедурой входа в систему | A.09.4.2 | ORG.4 | Инфраструктура и рабочая среда<br>6 Контролируется доступ к информационным ресурсам |
| Система управления паролями<br>1 Системы управления паролями должны быть диалоговыми и гарантировать пароли надлежащего качества | A.09.4.3 | ORG.4 | Инфраструктура и рабочая среда<br>6 Контролируется доступ к информационным ресурсам |
| Использование утилит с привилегированными правами<br>1 Применение утилит, которые могли бы обходить средства контроля системы и приложений, должно быть ограничено и жестко контролироваться | A.09.4.4 | ORG.4 | Инфраструктура и рабочая среда<br>2 Информационные ресурсы защищаются от нарушений |
| Контроль доступа к исходным кодам<br>1 Доступ к исходному коду программ должен быть ограничен | A.09.4.5 | ORG.4 | Инфраструктура и рабочая среда<br>6 Контролируется доступ к информационным ресурсам |
| Политика использования криптографических методов защиты<br>1 Должна быть разработана [и внедрена] политика использования криптографических методов защиты информации | A.10.1.1 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Политика использования криптографических методов защиты<br>2 Должна быть [разработана и] внедрена политика использования криптографических методов защиты информации | A.10.1.1 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Управление ключами<br>1 Политика использования, защиты и срока действия криптографических ключей должна быть разработана [и реализована] в течение всего жизненного цикла ключей | A.10.1.2 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Управление ключами<br>1 Политика использования, защиты и срока действия криптографических ключей должна быть [разработана и] реализована в течение всего жизненного цикла ключей | A.10.1.2 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Физический периметр безопасности<br>1 Периметры безопасности должны быть определены [и использованы] для защиты зон нахождения уязвимой или особо важной информации и средств для обработки информации | A.11.1.1 | ORG.4 | Инфраструктура и рабочая среда<br>1 Определяются требования к инфраструктуре и рабочей среде для поддержки процессов |
| Физический периметр безопасности<br>2 Периметры безопасности должны быть [определены и] использованы для защиты зон нахождения уязвимой или особо важной информации и средств для обработки информации | A.11.1.1 | ORG.4 | Инфраструктура и рабочая среда<br>5 Инфраструктура и рабочая среда контролируются и сопровождаются |
| Средства контроля прохода<br>1 Охраняемые зоны должны быть защищены соответствующими средствами контроля прохода с целью гарантировать, что только имеющему права персоналу разрешен доступ | A.11.1.2 | ORG.4 | Инфраструктура и рабочая среда<br>1 Определяются требования к инфраструктуре и рабочей среде для поддержки процессов |
| Защита офисов, помещений и устройств<br>1 Меры защиты для офисов, помещений и оборудования должны быть разработаны [и применены] | A.11.1.3 | ORG.4 | Инфраструктура и рабочая среда<br>1 Определяются требования к инфраструктуре и рабочей среде для поддержки процессов |
| Защита офисов, помещений и устройств<br>1 Меры защиты для офисов, помещений и оборудования должны быть [разработаны и] применены | A.11.1.3 | ORG.4 | Инфраструктура и рабочая среда<br>5 Инфраструктура и рабочая среда контролируются и сопровождаются |
| Защита от внешних угроз и угроз природного характера<br>1 Должны быть разработаны [и применяться] меры физической защиты от стихийных бедствий, злонамеренных действий или аварий | A.11.1.4 | ORG.4 | Инфраструктура и рабочая среда<br>1 Определяются требования к инфраструктуре и рабочей среде для поддержки процессов |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Защита от внешних угроз и угроз природного характера<br>2 Должны быть [разработаны и] применяться меры физической защиты от стихийных бедствий, злонамеренных действий или аварий | А.11.1.4 | ORG.4 | Инфраструктура и рабочая среда<br>5 Инфраструктура и рабочая среда контролируются и сопровождаются |
| Работа в охраняемых зонах<br>1 Должны быть разработаны [и применяться] процедуры для работы в охраняемой зоне | А.11.1.5 | COM.08 | Эксплуатационное планирование<br>3 Определяется множество действий, преобразующих входы в выходные результаты |
| Работа в охраняемых зонах<br>2 Должны быть [разработаны и] применяться процедуры для работы в охраняемой зоне | А.11.1.5 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Зоны доставки и отгрузки<br>1 Места доступа, такие как зоны доставки и отгрузки и иные, где есть возможность пройти в помещение лицам без соответствующих прав, должны контролироваться и, если возможно, быть изолированными от средств обработки информации, чтобы избежать несанкционированного доступа | А.11.1.6 | ORG.4 | Инфраструктура и рабочая среда<br>5 Инфраструктура и рабочая среда контролируются и сопровождаются |
| Размещение и защита оборудования<br>1 Оборудование должно быть размещено и защищено так, чтобы снизить риски, связанные с природными угрозами и опасностями, а также возможностью несанкционированного доступа | А.11.2.1 | ORG.2 | Управление оборудованием<br>1 Оборудование размещается так, чтобы минимизировать риски возникновения экологических и иных ущербов |
| Службы обеспечения<br>1 Оборудование должно быть защищено от перебоев в электроснабжении и других нарушений, вызванных перебоями в работе служб обеспечения | А.11.2.2 | ORG.2 | Управление оборудованием<br>2 Гарантируется непрерывность в обеспечении потребностей и обслуживания оборудования |
| Защита кабельных сетей<br>1 Питающие кабели и кабели, передающие данные или обеспечивающие работу информационных услуг, должны быть защищены от перехвата, помех или повреждения | А.11.2.3 | ORG.2 | Управление оборудованием<br>1 Оборудование размещается так, чтобы минимизировать риски возникновения экологических и иных ущербов |
| Обслуживание оборудования<br>1 Оборудование должно надлежащим образом обслуживаться, чтобы гарантировать его постоянную готовность и исправность | А.11.2.4 | ORG.2 | Управление оборудованием<br>3 Оборудование обслуживается для обеспечения непрерывной доступности и целостности |
| Перемещение активов<br>1 Оборудование, информация или программное обеспечение не должны выноситься за пределы территории без предварительного разрешения | А.11.2.5 | ORG.2 | Управление оборудованием<br>6 Контролируется перемещение оборудования |
| Защита оборудования и активов вне территории<br>1 Меры обеспечения безопасности должны применяться к активам вне территории, принимая во внимание различные риски работы вне помещений организации | А.11.2.6 | ORG.2 | Управление оборудованием<br>4 Осуществляется управление оборудованием, используемым за пределами организации, для обеспечения целостности его функционирования |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Безопасная утилизация или повторное использование оборудования<br>1 Все элементы оборудования, содержащие накопители, должны быть проверены, чтобы гарантировать, что любые ценные данные и лицензионное программное обеспечение удалены или надежным образом затерты новой информацией до утилизации или повторного использования | A.11.2.7 | ORG.2 | Управление оборудованием<br>5 Обеспечивается целостность информации, когда оборудование изымается из эксплуатации |
| Оборудование пользователя, оставленное без присмотра<br>1 Пользователи должны гарантировать, что у оставленного без присмотра оборудования имеется соответствующая защита | A.11.2.8 | ORG.4 | Инфраструктура и рабочая среда<br>5 Инфраструктура и рабочая среда контролируются и сопровождаются |
| Политика чистого стола и чистого экрана<br>1 Должна быть [адаптирована] политика чистого стола для бумажных документов и сменных носителей информации и политика чистого экрана для устройств обработки информации | A.11.2.9 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Политика чистого стола и чистого экрана<br>1 Должна быть адаптирована политика чистого стола для бумажных документов и сменных носителей информации и политика чистого экрана для устройств обработки информации | A.11.2.9 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Документируемые рабочие процедуры<br>1 Рабочие процедуры [должны быть документированы и доступны всем пользователям, которым они необходимы] | A.12.1.1 | COM.08 | Эксплуатационное планирование<br>3 Определяется множество действий, преобразующих входы в выходные результаты |
| Документируемые рабочие процедуры<br>2 [Рабочие процедуры] должны быть документированы [и доступны всем пользователям, которым они необходимы] | A.12.1.1 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Документируемые рабочие процедуры<br>2 [Рабочие процедуры должны быть документированы] и доступны всем пользователям, которым они необходимы | A.12.1.1 | COM.02 | Управление документацией<br>6 Документируемая информация становится доступной для заинтересованных сторон |
| Управление изменениями<br>1 Изменения в организации, бизнес-процессах, средствах для обработки информации и системах, которые влияют на информационную безопасность, должны быть управляемыми | A.12.1.2 | COM.09<br><br>COM.09 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления<br>Функциональная реализация и управление<br>5 При недостижении целей исправляются отклонения в планируемых действиях |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Управление возможностями<br>1 Использование ресурсов должно отслеживаться, регулироваться и делать прогноз требований к возможностям в будущем с тем, чтобы гарантировать необходимую работоспособность систем | А.12.1.3 | TEC.01 | Управление возможностями<br>3 Использование возможностей контролируется, анализируется и настраивается |
| Разделение среды разработки, тестирования и эксплуатации<br>1 Среда разработки, тестирования и рабочая среда должны быть отделены друг от друга для снижения рисков несанкционированного доступа или изменений в эксплуатационной среде | А.12.1.4 | ORG.4 | Инфраструктура и рабочая среда<br>2 Определяются права доступа к информационным ресурсам |
| Меры защиты от вредоносного кода<br>1 В отношении вредоносного кода должны применяться меры по обнаружению, предупреждению и восстановлению с соответствующим информированием пользователей | А.12.2.1 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Резервное копирование информации<br>1 Должно выполняться и регулярно [тестироваться резервное копирование информации, программного обеспечения и образов системы в соответствии с принятой политикой резервного копирования] | А.12.3.1 | TEC.09 | Сохранение и восстановление технических данных<br>3 Выполняется сохранение резервных копий |
| Резервное копирование информации<br>2 Должно [выполняться и регулярно] тестироваться [резервное копирование информации, программного обеспечения и образов системы в соответствии с принятой политикой резервного копирования] | А.12.3.1 | TEC.09 | Сохранение и восстановление технических данных<br>4 Выполняется восстановление данных |
| Резервное копирование информации<br>3 [Должно выполняться и] регулярно [тестироваться резервное копирование информации, программного обеспечения и образов системы в соответствии с принятой политикой резервного копирования] | А.12.3.1 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Резервное копирование информации<br>4 Должно выполняться и регулярно тестироваться резервное копирование информации, программного обеспечения и образов системы в соответствии с [принятой политикой резервного копирования] | А.12.3.1 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Регистрация событий<br>1 Должны вестись [сохраняться и регулярно анализироваться] журналы, содержащие записи активности пользователей, возникновения исключений, сбоев и событий, связанных с информационной безопасностью | А.12.4.1 | ORG.4 | Инфраструктура и рабочая среда<br>2 Информационные ресурсы защищаются от нарушений |
| Регистрация событий<br>2 Должны [вестись], сохраняться [и регулярно анализироваться] журналы, содержащие записи активности пользователей, возникновения исключений, сбоев и событий, связанных с информационной безопасностью | А.12.4.1 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Регистрация событий<br>3 Должны [вестись, сохраняться] и регулярно анализироваться журналы, содержащие записи активности пользователей, возникновения исключений, сбоев и событий, связанных с информационной безопасностью | A.12.4.1 | COM.09 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления |
| Защита информации в журналах<br>1 Средства для ведения журналов и внесенная в них информация должны быть защищены от несанкционированного вмешательства и несанкционированного доступа | A.12.4.2 | ORG.4 | Инфраструктура и рабочая среда<br>2 Информационные ресурсы защищаются от нарушений |
| Журналы действий администратора и оператора<br>1 Должны быть зафиксированы действия системных администраторов и операторов, [журналы должны быть защищены и регулярно анализироваться] | A.12.4.3 | ORG.4 | Инфраструктура и рабочая среда<br>6 Контролируется доступ к информационным ресурсам |
| Журналы действий администратора и оператора<br>2 [Должны быть зафиксированы действия системных администраторов и операторов,] журналы должны быть защищены [и регулярно анализироваться] | A.12.4.3 | ORG.4 | Инфраструктура и рабочая среда<br>6 Контролируется доступ к информационным ресурсам |
| Журналы действий администратора и оператора<br>3 Должны быть зафиксированы действия системных администраторов и операторов, журналы должны быть защищены [и регулярно анализироваться] | A.12.4.3 | COM.09<br><br><br><br><br><br>ORG.4 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления<br>Инфраструктура и рабочая среда<br>6 Контролируется доступ к информационным ресурсам |
| Синхронизация часов<br>1 Время у всех информационных систем, обрабатывающих важную информацию, в пределах организации или домена безопасности должно быть синхронизировано с единым источником эталонного времени | A.12.4.4 | ORG.4 | Инфраструктура и рабочая среда<br>1 Определяются требования к инфраструктуре и рабочей среде для поддержки процессов |
| Установка программ в эксплуатируемых системах<br>1 Должны быть [внедрены] процедуры для управления установкой программного обеспечения в эксплуатируемых системах | A.12.5.1 | COM.08 | Эксплуатационное планирование<br>3 Определяется множество действий, преобразующих входы в выходные результаты |
| Установка программ в эксплуатируемых системах<br>2 Должны быть внедрены процедуры для управления установкой программного обеспечения в эксплуатируемых системах | A.12.5.1 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Управление техническими уязвимостями<br>1 Должна своевременно получаться информация о технических уязвимостях в используемых информационных системах, должно оцениваться влияние этих уязвимостей на организацию и приниматься соответствующие меры для выработки реакции на риски, связанные с этим | A.12.6.1 | ORG.4 | Инфраструктура и рабочая среда<br>2 Информационные ресурсы защищаются от нарушений |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Ограничения на установку программных средств<br>1 Правила, регулирующие установку программного обеспечения пользователями, должны быть разработаны и внедрены | А.12.6.2 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Ограничения на установку программных средств<br>2 Правила, регулирующие установку программного обеспечения пользователями, должны быть разработаны [и внедрены] | А.12.6.2 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Контроль аудитов информационных систем<br>1 Требования и действия по аудиту, направленному на проверку эксплуатируемых систем, должны тщательно планироваться и [согласовываться] с целью минимизации нарушений нормального выполнения бизнес-процессов | А.12.7.1 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Средства аудитов информационных систем<br>1 Требования и действия по аудиту, направленному на проверку эксплуатируемых систем, должны [тщательно планироваться и] согласовываться с целью минимизации нарушений нормального выполнения бизнес-процессов | А.12.7.1 | COM.09 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления |
| Средства управления сетями<br>1 Сети должны управляться и контролироваться, чтобы защитить информацию в системах и приложениях | А.13.1.1 | ORG.2 | Управление оборудованием<br>3 Оборудование обслуживается для обеспечения непрерывной доступности и целостности |
| Безопасность сетевых услуг<br>1 Должны быть определены для всех сетевых услуг и включены в соглашения по обслуживанию сетей механизмы обеспечения безопасности, уровни услуг и требования к управлению, осуществляются ли эти услуги внутренними подразделениями или сторонней организацией | А.13.1.2 | ORG.4 | Инфраструктура и рабочая среда<br>1 Определяются требования к инфраструктуре и рабочей среде для поддержки процессов |
| Разделение в сетях<br>1 Различные группы информационных служб, пользователей и информационных систем должны быть разделены в сетях | А.13.1.3 | ORG.4 | Инфраструктура и рабочая среда<br>2 Определяются права доступа к информационным ресурсам |
| Политики и процедуры передачи информации<br>1 Должны быть разработаны политики, [процедуры и средства] управления для защиты передачи информации, осуществляемой посредством любых типов оборудования связи | А.13.2.1 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Политики и процедуры передачи информации<br>2 Должны быть разработаны [политики], процедуры и средства управления для защиты передачи информации, осуществляемой посредством любых типов оборудования связи | А.13.2.1 | COM.08 | Эксплуатационное планирование<br>3 Определяется множество действий, преобразующих входы в выходные результаты |
| Соглашения по передаче информации<br>1 Соглашения должны регламентировать безопасную передачу деловой информации между организацией и внешними сторонами | А.13.2.2 | ORG.5 | Управление поставщиками<br>2 Обеспечивающие продукция/услуги обговариваются и определяются с каждым поставщиком |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Электронные сообщения<br>1 Информация, передаваемая электронными сообщениями, должна быть соответствующим образом защищена | A.13.2.3 | ORG.4 | Инфраструктура и рабочая среда<br>2 Информационные ресурсы защищаются от нарушений |
| Соглашения о конфиденциальности или неразглашении<br>1 Требования к соглашениям о конфиденциальности или неразглашении, отражающие потребности организации в защите информации, должны быть определены, документированы и регулярно анализироваться | A.13.2.4 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Соглашения о конфиденциальности или неразглашении<br>2 Требования к соглашениям о конфиденциальности или неразглашении, отражающие потребности организации в защите информации, должны [быть определены], документированы и [регулярно анализироваться] | A.13.2.4 | COM.09 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления |
| Соглашения о конфиденциальности или неразглашении<br>3 Требования к соглашениям о конфиденциальности или неразглашении, отражающие потребности организации в защите информации, должны [быть определены], документированы и [регулярно анализироваться] | A.13.2.4 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Анализ и установление требований по информационной безопасности<br>1 Требования, связанные с информационной безопасностью, должны быть включены в требования для новых информационных систем или расширения к существующим информационным системам | A.14.1.1 | TEC.08 | Продукция/ услуги/ системные требования<br>3 Определяются требования к продукции/ услугам/ системе |
| Безопасность прикладных услуг в сетях общего пользования<br>1 Информация, используемая прикладными услугами, передающаяся по общедоступным сетям, должна быть защищена от мошеннических действий, претензий, связанных с нарушениями контрактных обязательств, и несанкционированного раскрытия и изменения | A.14.1.2 | TEC.08 | Продукция/ услуги/ системные требования<br>3 Определяются требования к продукции/ услугам/ системе |
| Защита операций прикладных услуг<br>1 Информация, участвующая в операциях, осуществляемых при пользовании прикладными услугами, должна быть защищена с целью предотвращения незавершенной передачи, неправильной маршрутизации, несанкционированного изменения сообщения, несанкционированного раскрытия, несанкционированного дублирования сообщения или воспроизведения | A.14.1.3 | ORG.4 | Инфраструктура и рабочая среда<br>2 Информационные ресурсы защищаются от нарушений |
| Политика безопасности при разработке<br>1 Правила для разработки программного обеспечения и систем должны быть установлены и применяться ко всем разработкам в организации | A.14.2.1 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Процедуры управления системными изменениями<br>1 Изменения в системах в течение цикла разработки должны быть управляемыми посредством формализованных процедур управления изменениями | А.14.2.2 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Технический анализ приложений после изменений операционной платформы<br>1 После изменения операционной платформы критичные бизнес-приложения должны быть проанализированы и протестированы для гарантий того, что отсутствует негативное влияние на деятельность организации или безопасность | А.14.2.3 | COM.09<br><br><br><br><br>TEC.05<br><br><br><br>TEC.08 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления<br>Производство продукции/ оказание услуг<br>5 Осуществляются проверки в соответствии с определенными критериями<br>Продукция/ услуги/ системные требования<br>3 Определяются требования к продукции/ услугам/ системе |
| Ограничения на изменения в пакетах программ<br>1 Модификация пакетов программ не должна поощряться и должна быть ограничена только необходимыми изменениями, а все изменения должны строго контролироваться | А.14.2.4 | TEC.03 | Управление конфигурацией<br>3 Контролируются изменения в объектах в рамках управления конфигурацией |
| Принципы безопасной системной инженерии<br>1 Принципы безопасной системной инженерии должны быть установлены [документированы, поддерживаться] и применяться во всех случаях внедрения информационных систем | А.14.2.5 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Принципы безопасной системной инженерии<br>1 Принципы безопасной системной инженерии должны быть [установлены], документированы, [поддерживаться и применяться во всех случаях внедрения информационных систем] | А.14.2.5 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Принципы безопасной системной инженерии<br>1 Принципы безопасной системной инженерии должны быть [установлены, документированы], поддерживаться и [применяться во всех случаях внедрения информационных систем] | А.14.2.5 | COM.02 | Управление документацией<br>3 Становится известным статус содержания документируемой информации |
| Безопасная среда разработки<br>1 Организации должны обеспечивать и соответствующим образом защищать безопасные среды разработки и интеграции систем, охватывающие весь цикл разработки | А.14.2.6 | ORG.4 | Инфраструктура и рабочая среда<br>1 Определяются требования к инфраструктуре и рабочей среде для поддержки процессов |
| Разработка, переданная на аутсорсинг<br>1 Организация должна контролировать и вести мониторинг процесса разработки системы, переданного на аутсорсинг | А.14.2.7 | COM.09 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Тестирование безопасности системы<br>1 В ходе разработки должно выполняться тестирование функциональности, связанной с безопасностью | А.14.2.8 | СОМ.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Приемочное тестирование системы<br>1 Должно быть выбрано тестовое программное обеспечение и установлены критерии приемки для новых информационных систем, обновлений и новых версий | А.14.2.9 | ТЕС.08 | Продукция/ услуги/ системные требования<br>4 Определяются требования к валидации (аттестации) продукции/ услуг/ системы |
| Защита данных для тестирования<br>1 Данные для тестирования должны тщательно выбираться, быть защищенными и контролироваться | А.14.3.1 | ТЕС.03 | Управление конфигурацией<br>3 Контролируются изменения в объектах в рамках управления конфигурацией |
| Политика информационной безопасности в отношениях с поставщиками<br>1 Требования по информационной безопасности для снижения рисков, связанных с доступом поставщиков к активам организации [должны быть согласованы с поставщиками и документированы] | А.15.1.1 | СОМ.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |
| Политика информационной безопасности в отношениях с поставщиками<br>2 Требования по информационной безопасности [для снижения рисков, связанных с доступом поставщиков к активам организации], должны быть согласованы с поставщиками [и документированы] | А.15.1.1 | СОМ.02 | Управление документацией<br>5 Доводится по определенным критериям документируемая информация |
| Политика информационной безопасности в отношениях с поставщиками<br>1 Требования по информационной безопасности [для снижения рисков, связанных с доступом поставщиков к активам организации, должны быть согласованы с поставщиками] и документированы | А.15.1.1 | СОМ.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Решение вопросов безопасности в соглашениях с поставщиками<br>1 Все существенные требования по информационной безопасности должны быть установлены и согласованы с каждым поставщиком, который может получать доступ, обрабатывать, хранить, передавать информацию организации или поставлять компоненты для ИТ-инфраструктуры | А.15.1.2 | ORG.5 | Управление поставщиками<br>2 Обеспечивающие продукция/ услуги обговариваются и определяются с каждым поставщиком |
| Цепочка поставок информационно-коммуникационных технологий<br>1 Соглашения с поставщиками должны включать требования, учитывающие риски информационной безопасности, связанные с цепочкой поставок услуг и продуктов в сфере информационно-коммуникационных технологий | А.15.1.3 | ORG.5 | Управление поставщиками<br>2 Обеспечивающие продукция/ услуги обговариваются и определяются с каждым поставщиком |
| Контроль и анализ услуг поставщика<br>1 Организации должны регулярно отслеживать, анализировать и [проводить аудит] предоставления услуг поставщиком | А.15.2.1 | СОМ.09 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Контроль и анализ услуг поставщика<br>1 Организации должны регулярно [отслеживать, анализировать] и проводить аудит предоставления услуг поставщиком | А.15.2.1 | COM.05 | Внутренний аудит<br>3 Определяется соответствие выбранных услуг, продукции и процессов требованиям, планам и соглашениям |
| Контроль и анализ услуг поставщика<br>1 Организации должны регулярно [отслеживать, анализировать и проводить аудит предоставления услуг поставщиком] | А.15.2.1 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Управление изменениями в услугах поставщика<br>1 Необходимо управлять изменениями в предоставлении услуг поставщиками, включая поддержание и улучшение существующих политик информационной безопасности, процедур и средств управления, с учетом критичности деловой информации, используемых систем и процессов, и повторной оценки рисков | А.15.2.2 | TEC.02 | Управление изменениями<br>2 Заявки на изменения анализируются и оцениваются по определенным критериям |
| Ответственность и процедуры<br>1 Должны быть установлены ответственность руководства [и процедуры], чтобы гарантировать быстрый, результативный и надлежащий ответ на инциденты нарушения информационной безопасности | А.16.1.1 | COM.08 | Эксплуатационное планирование<br>5 Определяются необходимые компетенции и функции для выполнения процесса |
| Ответственность и процедуры<br>2 Должны быть установлены [ответственность руководства] и процедуры, чтобы гарантировать быстрый, результативный и надлежащий ответ на инциденты нарушения информационной безопасности | А.16.1.1 | COM.08 | Эксплуатационное планирование<br>3 Определяется множество действий, преобразующих входы в выходные результаты |
| Оповещение о событиях, связанных с информационной безопасностью<br>1 Оповещение о событиях информационной безопасности должно доводиться по соответствующим каналам управления как можно быстрее | А.16.1.2 | TEC.04 | Управление инцидентами<br>1 Определяются инциденты |
| Оповещение об уязвимостях в информационной безопасности<br>1 От сотрудников и работающих по контракту, использующих информационные системы и услуги организации, необходимо требовать фиксировать и докладывать о любых обнаруженных или предполагаемых уязвимостях в информационной безопасности систем и услуг | А.16.1.3 | TEC.04 | Управление инцидентами<br>1 Определяются инциденты |
| Оценка и решение по событиям информационной безопасности<br>1 События информационной безопасности должны оцениваться и затем принимается решение, следует ли их классифицировать как инцидент нарушения информационной безопасности | А.16.1.4 | TEC.04 | Управление инцидентами<br>2 Инциденты классифицируются, располагаются по приоритетам и анализируются |
| Реагирование на инциденты нарушения информационной безопасности<br>1 Реагирование на инциденты нарушения информационной безопасности должно осуществляться [в соответствии с документированными процедурами] | А.16.1.5 | TEC.04 | Управление инцидентами<br>3 Инциденты разрешаются и закрываются |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Реагирование на инциденты нарушения информационной безопасности<br>2 Реагирование на инциденты нарушения информационной безопасности должно осуществляться в соответствии с [документированными] процедурами | A.16.1.5 | COM.08 | Эксплуатационное планирование<br>3 Определяется множество действий, преобразующих входы в выходные результаты |
| Реагирование на инциденты нарушения информационной безопасности<br>3 Реагирование на инциденты нарушения информационной безопасности [должно осуществляться в соответствии с] документированными [процедурами] | A.16.1.5 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Извлечение уроков из инцидентов нарушения информационной безопасности<br>1 Знания, полученные из анализа и разрешения инцидентов нарушения информационной безопасности, должны использоваться для уменьшения вероятности инцидентов в будущем или их воздействия | A.16.1.6 | COM.10 | Оценка функционирования<br>5 Анализируются собираемые данные о функционировании |
| Сбор свидетельств<br>1 [Организация должна определить и применять процедуры для идентификации, сбора, комплектования и сохранения информации], которая может служить в качестве свидетельств | A.16.1.7 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Сбор свидетельств<br>2 Организация должна определить [и применять] процедуры для идентификации, сбора, комплектования и сохранения информации [которая может служить в качестве свидетельств] | A.16.1.7 | COM.08 | Эксплуатационное планирование<br>3 Определяется множество действий, преобразующих входы в выходные результаты |
| Сбор свидетельств<br>3 Организация должна [определить] и применять процедуры для идентификации, сбора, комплектования и сохранения информации [которая может служить в качестве свидетельств] | A.16.1.7 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Планирование непрерывности информационной безопасности<br>1 Организация должна определить свои требования к информационной безопасности и управлению непрерывностью информационной безопасности в неблагоприятных ситуациях, например во время кризиса или чрезвычайной ситуации | A.17.1.1 | TEC.07 | Управление непрерывностью услуг<br>1 Определяются требования к непрерывности в оказании услуг |
| Обеспечение непрерывности информационной безопасности<br>1 Организация должна установить [документировать], внедрить и [поддерживать] процессы, процедуры и средства управления, чтобы гарантировать необходимый уровень непрерывности информационной безопасности во время неблагоприятной ситуации | A.17.1.2 | COM.08 | Эксплуатационное планирование<br>1 Определяются потребности и требования процесса |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Обеспечение непрерывности информационной безопасности<br>2 Организация должна установить [документировать], внедрить и [поддерживать] процессы, процедуры и средства управления, чтобы гарантировать необходимый уровень непрерывности информационной безопасности во время неблагоприятной ситуации | A.17.1.2 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Обеспечение непрерывности информационной безопасности<br>3 Организация должна [установить], документировать [внедрить и поддерживать процессы, процедуры и средства управления, чтобы гарантировать необходимый уровень непрерывности информационной безопасности во время неблагоприятной ситуации] | A.17.1.2 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Обеспечение непрерывности информационной безопасности<br>4 Организация должна [установить, документировать, внедрить] и поддерживать [процессы, процедуры и средства управления, чтобы гарантировать необходимый уровень непрерывности информационной безопасности во время неблагоприятной ситуации] | A.17.1.2 | COM.02 | Управление документацией<br>3 Становится известным статус содержания документируемой информации |
| Верификация, анализ и оценка непрерывности информационной безопасности<br>1 Организация должна проверять разработанные и внедренные средства управления непрерывностью информационной безопасности [через определенные интервалы времени], чтобы гарантировать, что эти средства пригодны и результативны во время неблагоприятных ситуаций | A.17.1.3 | COM.09<br><br><br><br><br>TEC.07 | Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления<br>Управление непрерывностью услуг<br>3 Непрерывность услуг оценивается по требованиям, предъявляемым к непрерывности услуг |
| Верификация, анализ и оценка непрерывности информационной безопасности<br>1 Организация должна проверять разработанные и внедренные средства управления непрерывностью информационной безопасности [через определенные интервалы времени], чтобы гарантировать, что эти средства пригодны и результативны во время неблагоприятных ситуаций | A.17.1.3 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Возможность применения средств обработки информации<br>1 Средства обработки информации должны устанавливаться с избыточностью, достаточной для обеспечения требований по возможности применения | A.17.2.1 | COM.09<br><br><br><br>TEC.06 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления<br>Управление готовностью услуг<br>1 Определяются требования к готовности оказания услуг |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Применяемые законодательные и нормативные требования<br>1 Все соответствующие законодательные, нормативные [контрактные] требования, а также подход организации к удовлетворению этих требований должны быть явным образом определены [документированы и сохраняться актуальными для каждой информационной системы и организации] | A.18.1.1.01 | TEC.08 | Продукция/ услуги/ системные требования<br>3 Определяются требования к продукции/ услугам/ системе |
| Прикладные законодательные и нормативные требования<br>2 Все соответствующие законодательные, нормативные [контрактные] требования, а также подход организации к удовлетворению этих требований должны быть [явным образом определены], документированы [и сохраняться актуальными для каждой информационной системы и организации] | A.18.1.1.01 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Прикладные законодательные и нормативные требования<br>3 Все соответствующие законодательные, нормативные [контрактные] требования, а также подход организации к удовлетворению этих требований должны быть явным образом [определены, документированы и] сохраняться актуальными для каждой информационной системы и организации | A.18.1.1.01 | COM.02 | Управление документацией<br>3 Становится известным статус содержания документируемой информации |
| Применяемые контрактные требования<br>1 Все соответствующие [законодательные, нормативные], контрактные требования, а также подход организации к удовлетворению этих требований должны быть [явным образом определены] документированы [и сохраняться актуальными для каждой информационной системы и организации] | A.18.1.1.02 | TEC.08 | Продукция/ услуги/ системные требования<br>3 Определяются требования к продукции/ услугам/ системе |
| Применяемые контрактные требования<br>2 Все соответствующие [законодательные, нормативные], контрактные требования, а также подход организации к удовлетворению этих требований должны быть [явным образом определены], документированы [и сохраняться актуальными для каждой информационной системы и организации] | A.18.1.1.02 | COM.02 | Управление документацией<br>1 Определяется документируемая информация для управления |
| Применяемые контрактные требования<br>3 Все соответствующие [законодательные, нормативные], контрактные требования, а также подход организации к удовлетворению этих требований должны быть [явным образом определены, документированы и] сохраняться актуальными для каждой информационной системы и организации | A.18.1.1.02 | COM.02 | Управление документацией<br>3 Становится известным статус содержания документируемой информации |
| Права интеллектуальной собственности<br>1 [Должны выполняться] соответствующие процедуры, чтобы гарантировать соответствие законодательным, нормативным и контрактным требованиям, связанным с правами на интеллектуальную собственность и использованием программных продуктов, защищенных авторским правом | A.18.1.2 | COM.08 | Эксплуатационное планирование<br>3 Определяется множество действий, преобразующих входы в выходные результаты |

*Продолжение таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Права интеллектуальной собственности<br>2 Должны выполняться соответствующие процедуры, чтобы гарантировать соответствие законодательным, нормативным и контрактным требованиям, связанным с правами на интеллектуальную собственность и использованием программных продуктов, защищенных авторским правом | А.18.1.2 | COM.09 | Функциональная реализация и управление<br>3 Реализуются действия, востребованные для достижения целей системы управления |
| Защита записей<br>1 Записи должны быть защищены от потери, повреждения, фальсификации, несанкционированного доступа и несанкционированной публикации в соответствии с законодательными, нормативными, контрактными требованиями и требованиями бизнеса | А.18.1.3 | COM.02 | Управление документацией<br>4 Документируемая информация является обновляемой, полной и достоверной |
| Конфиденциальность и защита персональных данных<br>1 Конфиденциальность и защита персональных данных должны быть обеспечены в той мере, в какой это требуется соответствующим законодательством и нормативными актами, где это применимо | А.18.1.4 | ORG.4 | Инфраструктура и рабочая среда<br>2 Информационные ресурсы защищаются от нарушений |
| Регламентация применения криптографических методов<br>1 Криптографические методы должны использоваться в соответствии со всеми действующими соглашениями, законодательными и нормативными актами | А.18.1.5 | ORG.4 | Инфраструктура и рабочая среда<br>2 Информационные ресурсы защищаются от нарушений |
| Независимый анализ информационной безопасности<br>1 Подход организации к управлению информационной безопасностью и его реализация (т. е. задачи управления, средства управления, политики, процессы и процедуры по обеспечению информационной безопасности) должны подвергаться независимому анализу [через запланированные интервалы времени или в тех случаях, когда происходят существенные изменения] | А.18.2.1 | COM.05<br><br><br><br>COM.09 | Внутренний аудит<br>3 Определяется соответствие выбранных услуг, продукции и процессов требованиям, планам и соглашениям<br>Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления |
| Независимый анализ информационной безопасности<br>2 [Подход организации к управлению информационной безопасностью и его реализация (т. е. задачи управления, средства управления, политики, процессы и процедуры по обеспечению информационной безопасности) должны подвергаться независимому анализу через запланированные интервалы времени или в тех случаях, когда происходят существенные изменения] | А.18.2.1 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |

*Окончание таблицы А.2*

| ИСО/МЭК 27001:2013 | | Обобщенные процессы управления | |
|---|---|---|---|
| Соответствие политикам безопасности и стандартам<br>1 Руководители в пределах своей области ответственности должны [регулярно] анализировать соответствие обработки информации и процедур политикам безопасности, стандартам и любым другим требованиям по безопасности | A.18.2.2 | COM.05<br><br><br><br><br>COM.09 | Внутренний аудит<br>3 Определяется соответствие выбранных услуг, продукции и процессов требованиям, планам и соглашениям<br>Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления |
| Соответствие политикам безопасности и стандартам<br>2 Руководители в пределах своей области ответственности должны регулярно [анализировать] соответствие обработки информации и процедур политикам безопасности, стандартам и любым другим требованиям по безопасности | A.18.2.2 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |
| Анализ технического соответствия<br>1 Информационные системы должны [регулярно] анализироваться на соответствие политикам и стандартам информационной безопасности организации | A.18.2.3 | COM.05<br><br><br>COM.09 | Внутренний аудит<br>1 Определяется область проведения и цель каждого аудита<br>Функциональная реализация и управление<br>4 Анализируются пригодность и эффективность действий, предпринятых для достижения целей системы управления |
| Анализ технического соответствия<br>1 Информационные системы должны регулярно [анализироваться на соответствие политикам и стандартам информационной безопасности организации] | A.18.2.3 | COM.08 | Эксплуатационное планирование<br>8 Разрабатываются планы для исполнителей процесса |

**Приложение В**
**(справочное)**

## Положения по соответствию ИСО/МЭК 33004

### В.1 Общее

ЭМП в настоящем стандарте является пригодной для использования оценки процесса, выполняемой в соответствии с ИСО/МЭК 33004.

В ИСО/МЭК 33004:2015 (подраздел 5.3) приведены требования для ЭМП, пригодной для оценки процесса согласно ИСО/МЭК 33002. Настоящий стандарт устанавливает требования для ЭМП и описывает, как стандарт удовлетворяет этим требованиям. В каждом из следующих подразделов текст, представленный в рамке, приведен из ИСО/МЭК 33004, а текст, расположенный ниже рамки, описывает требования, которым отвечает настоящий стандарт.

#### В.1.1 Требования для ЭМП

**ИСО/МЭК 33004 Информационные технологии. Оценка процесса.**
**Требования к эталонным моделям процесса, моделям оценки процесса и моделям зрелости**

5.3.1 Эталонная модель процесса должна содержать:

a) декларацию области применения ЭМП;

b) описание отношений между эталонной моделью процесса и ее намеченным контекстом использования;

c) описания процессов в рамках эталонных моделей процесса согласно требованиям подраздела 5.4;

d) описание отношений между процессами, определенными в пределах ЭМП.

- Описание области — управление информационной безопасности.
- Описание процессов приведено в разделе 5 настоящего стандарта.
- ЭМП предназначена для использования, как описано во введении к настоящему стандарту.
- Описание отношений между процессами, определенными в пределах ЭМП, поддерживаются в соответствии с рисунком 2 настоящего стандарта.

**ИСО/МЭК 33004 Информационные технологии. Оценка процесса.**
**Требования к эталонным моделям процесса, моделям оценки процесса и моделям зрелости**

5.3.2 Эталонная модель процесса должна обеспечить документирование множества интересов со стороны конкретной модели и действий, предпринимаемых для достижения соответствия, а именно:

a) соответствующее множество интересов должно быть описано с использованием различных характеристик или задано;

b) степень достижения соответствия должна быть задокументирована;

c) если для достижения соответствия не предпринимается никаких действий, то это также должно быть задокументировано.

- Соответствующие сообщества по интересам и способы их использования ЭМП приведены во введении к настоящему стандарту.
- Настоящий стандарт удовлетворяет критериям консенсуса, принятым в ИСО/МЭК СТК1.
- Поскольку было достигнуто согласие, никаких дополнительных действий не требуется.

**ИСО/МЭК 33004 Информационные технологии. Оценка процесса.**
**Требования к эталонным моделям процесса, моделям оценки процесса и моделям зрелости**

5.3.3 У процессов, определенных в пределах ЭМП, должны быть уникальные идентификация и описания.

- Описания процесса уникальны. Идентификация предоставлена уникальным названием и идентификатором каждого процесса по настоящему стандарту.

**В.1.2 Описание процесса**

**ИСО/МЭК 33004 Информационные технологии. Оценка процесса.**

**Требования к эталонным моделям процесса, моделям оценки процесса и моделям зрелости**

5.4 Описания процесса

Основные элементы ЭМП — это описания процессов в рамках области применения модели.

Описания процесса в ЭМП включают в себя определение цели процесса, описывающей на высоком уровне обобщенные задачи выполнения процесса вместе с множеством выходных результатов, демонстрирующих успешное достижение этой цели.

Описание процесса должно отвечать следующим требованиям:

a) процесс должен быть описан в терминах его цели и результатов;

b) множество результатов процесса должно быть необходимым и достаточным для достижения цели процесса;

c) описания процесса не должны содержать или подразумевать аспекты характеристик качества процесса вне главного уровня любой соответствующей системы измерения процесса по ИСО/МЭК 33003.

Выходные результаты процесса описывают что-то одно из следующего:

- производство артефакта;
- существенное изменение состояния;
- удовлетворение заданных ограничений, например требований, целей и т. д.

- Этим требованиям отвечают описания процесса в разделе 5 настоящего стандарта.

## Приложение ДА
(справочное)

### Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

| Обозначение ссылочного международного стандарта | Степень соответствия | Обозначение и наименование соответствующего национального стандарта |
|---|---|---|
| ISO/IEC 27001:2013 | — | * |
| ISO/IEC 33001:2015 | — | * |

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде стандартов.

## Библиография


[1] ISO 9000:2015, Quality management systems — Fundamentals and vocabulary

[2] ISO 9001:2015, Quality management systems — Requirements

[3] ISO/IEC TR 24774:2010, Systems and software engineering — Life cycle management — Guidelines for process description

[4] ISO/IEC 33002:2015, Information technology — Process assessment — Requirements for performing process assessment

[5] ISO/IEC 33020:2015, Information technology — Process assessment — Process measurement framework for assessment of process capability

[6] ISO/IEC 33004:2015, Information technology — Process assessment — Requirements for process reference, process assessment and maturity models

УДК 004:006.34 ОКС 35.080 IDT

Ключевые слова: эталонная модель процесса (ЭМП), модели оценки процесса (МОП), система управления информационной безопасностью (СУИБ), описание процесса, защита информации

**БЗ 8—2017/23**

Редактор *К.В. Колесникова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Ю. Митрофанова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 07.09.2017. Подписано в печать 03.10.2017. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 7,91. Уч.-изд. л. 7,15. Тираж 23 экз. Зак. 1685.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123001 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru