ГОСТ Р 53647.6-2012 Менеджмент непрерывности бизнеса. Требования к системе менеджмента персональной информации для обеспечения защиты данных

ГОСТ Р 53647.6-2012

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ НЕПРЕРЫВНОСТИ БИЗНЕСА

Требования к системе менеджмента персональной информации для обеспечения защиты данных

Business continuity management. Specification for a personal information management system for data protection

ОКС 03.100.01

Дата введения 2013-12-01

Предисловие

1 ПОДГОТОВЛЕН Автономной некоммерческой организацией "Научно-исследовательский центр контроля и диагностики технических систем" (АНО "НИЦ КД") на основе собственного аутентичного перевода международного стандарта, указанного в разделе 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 10 "Менеджмент риска"

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 ноября 2012 г. N 1421-ст

4 Настоящий стандарт соответствует основным положениям национального стандарта Великобритании BS 10012:2009* "Защита данных. Требования к системе менеджмента персональной информации" (BS 10012:2009 "Data protection - Specification for a personal information management system").

---

* Доступ к международным и зарубежным документам, упомянутым здесь и далее по тексту, можно получить, перейдя по ссылке на сайт http://shop.cntd.ru. - Примечание изготовителя базы данных.

Наименование настоящего стандарта изменено относительно наименования указанного национального стандарта для приведения в соответствие с ГОСТ Р 1.5-2004 (подраздел 3.5).

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0-2012 (раздел 8). 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 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 (gost.ru)

Введение

0.1 Система менеджмента персональной информации

Применение настоящего стандарта может позволить организациям внедрить в рамках общей структуры управления информацией систему менеджмента персональной информации (СМПИ), которая служит основой повышения степени соответствия законодательным и обязательным требованиям о защите данных и передовому опыту в данной области деятельности.

Основным законом в этой сфере является Федеральный закон о защите персональных данных N 152 от 27.07.2006 г. [1]. Он реализует положения Конституции РФ и Европейской директивы 95/46/ЕС от 24 октября 1995 года [2] и применяется к "персональным данным", которые определены как любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), такая как его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация.

В настоящем стандарте термин "персональная информация" используется в качестве

синонима термину "персональные данные". В качестве синонимов термина "менеджмент персональной информации" часто используют термины "менеджмент персональных данных", "управление персональной информацией", "управление персональными данными". Выбор терминов зависит от потребностей организации и требований ее причастных сторон.

Закон о защите персональных данных регулируется и приводится в исполнение уполномоченным органом по защите прав субъектов персональных данных (далее - уполномоченный орган), ответственным за содействие защите персональной информации. Уполномоченный орган распространяет передовой мировой опыт путем опубликования руководств, правил по правомерным претензиям, предоставляет необходимую информацию физическим лицам и организациям, а также принимает соответствующие меры в случае нарушения закона.

Уполномоченный орган обладает полномочиями по расследованию претензий, проведению оценки соответствия обработки информации требованиям [1], выпуску информационных сообщений и уведомлений о принудительном исполнении требований законодательства.

0.2 Принципы защиты персональной информации

В соответствии с мировой практикой операторы, работающие с персональными данными, должны соблюдать восемь принципов защиты персональной информации, согласно которым персональная информация должна:

1-ый принцип - быть обработана квалифицированно и с учетом законодательных и обязательных требований;

2-ой принцип - быть собрана только для определенных целей и обработана только в соответствии с этими целями;

3-ий принцип - быть адекватной, соответствующей целям и не избыточной;

4-ый принцип - быть достоверной и актуальной;

5-ый принцип - не должна храниться больше установленного срока;

6-ой принцип - быть обработана с соблюдением законных прав физических лиц, включая право на получение доступа к личной информации;

7-ой принцип - быть защищена;

8-ой принцип - не должна передаваться в страны, находящиеся за пределами РФ, без обеспечения надлежащей защиты.

Из данных принципов защиты данных могут быть сделаны исключения. Большая часть таких исключений составляет следующие категории:

- исключения из принципа неразглашения;

- исключения из положений о предоставлении информации субъекту персональных данных;

- исключения, относящиеся к обработке информации в исторических и (или) исследовательских целях;

- прочие исключения, например, конфиденциальные ссылки и экзаменационные работы.

Дополнительная информация приведена в [1], инструкциях уполномоченного органа и в прочих руководствах и рекомендациях.

0.3 Уведомление

С целью обеспечения открытости в соответствие с [1] организация должна уведомлять уполномоченный орган об обработке персональной информации, за исключением случаев применения исключений в отношении уведомлений.

1 Область применения

Настоящий стандарт устанавливает требования к системе менеджмента персональной информации (СМПИ), направленные на обеспечение выполнения законодательных и обязательных требований по защите персональной информации, а также внедрения передового мирового опыта в этой области.

Примечание - Ко всем процессам СМПИ применяется цикл PDCA (планирование-осуществление-проверка-действие) (см. приложение А).

Настоящий стандарт применим к организациям разных размеров и форм собственности, и может быть использован лицами, ответственными за разработку, внедрение и поддержание в рабочем состоянии процессов СМПИ организации. Настоящий стандарт применяется при управлении персональной информацией, в том числе при обеспечении ее достоверности, а также при проведении внутренней и внешней оценки соответствия законодательным и обязательным требованиям в области защиты информации и передовому опыту.

2 Термины, определения и обозначения

2.1 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

2.1.1 **аудит** (audit): Систематический, независимый и документированный процесс получения свидетельств аудита (проверки) и объективного их оценивания с целью установления степени выполнения согласованных критериев аудита.

[ГОСТ Р ИСО 9000-2008]

Примечание - Внутренние аудиты, иногда называемые аудиты первой стороной, проводятся обычно самой организацией или от ее имени для внутренних целей и могут служить основанием для декларации о соответствии.

2.1.2 **физическое лицо** (individual): Лицо, являющееся субъектом персональных данных.

2.1.3 **система менеджмента** (management system): Система для разработки политики и целей и достижения этих целей.

[ГОСТ Р ИСО 9000-2008]

2.1.4 **несоответствие** (nonconformity): Невыполнение требования.

[ГОСТ Р ИСО 9000-2008, ГОСТ Р ИСО 14001-2007]

2.1.5 **организация** (organization): Группа работников и необходимых средств с указанием распределения ответственности, полномочий и взаимоотношений.

Примеры - Компания, корпорация, фирма, предприятие, учреждение, благотворительная организация, предприятие торговли, ассоциация, а также их подразделения или комбинации из них.

2.1.6 **персональная информация** (personal information): Информация, относящаяся к определенному физическому лицу, по которой его можно идентифицировать.

2.1.7 **политика менеджмента персональной информации** (personal information management policy): Официально оформленное и утвержденное высшим руководством заявление об общих намерениях и направлении развития организации в области защиты персональной информации, в том числе соответствии законодательным и обязательным требованиям и передовому опыту.

2.1.8 **система менеджмента персональной информации, СМПИ** (personal information management system, PIMS): Часть общей системы менеджмента, направленная на создание, внедрение, функционирование, мониторинг, анализ, поддержание в рабочем состоянии и постоянное улучшение менеджмента персональной информации.

2.1.9 **процедура** (procedure): Установленный способ осуществления деятельности или процесса, которые могут быть документированными и недокументированными.

2.1.10 **процесс** (process): Набор действий, направленных на достижение результата.

2.1.11 **обработка** (processing): Получение, запись, хранение и иные виды операций с персональной информацией.

Примечание - В понятие "обработка" входит сбор, организация, адаптация, изменение, раскрытие, обмен, распространение, согласование, объединение, блокирование, удаление и уничтожение персональной информации.

2.1.12 **персональная информация особой ответственности** (sensitive personal information): Персональная информация о:

a) национальности или отношении к этнической группе;

b) политических взглядах;

c) вероисповедании;

d) членстве в профсоюзе;

e) физическом или психическом здоровье или состоянии;

f) сексуальной ориентации;

g) правонарушениях, включая судебные разбирательства, прекращение судебного разбирательства, приговоры суда, вынесенные в ходе судебного разбирательства за правонарушение, совершенных или предполагаемых.

2.1.13 **система** (system): Совокупность взаимосвязанных и взаимодействующих элементов.

[ГОСТ Р ИСО 9000-2008]

2.1.14 **работники** (workers): Люди, работающие в организации и на нее.

Примечание - К работникам, работающим на организацию, могут быть отнесены

постоянный и временный персонал организации, подрядчики, добровольцы и консультанты.

2.2 Сокращения

PDCA	Планирование, осуществление, проверка, действие.
PIMS	Система менеджмента персональной информации (СМПИ).

_____

PDCA - Plan-Do-Check-Act.

PIMS - Personal Information management system.

3 Планирование СМПИ

Цель: Планирование внедрения системы менеджмента персональной информации, определяющей направления развития системы, и обеспечивающее соответствие передовому опыту в области защиты персональных данных и соблюдение законодательных и обязательных требований.

3.1 Создание и управление СМПИ

Организация должна разработать, задокументировать, внедрить, поддерживать в рабочем состоянии и постоянно улучшать СМПИ с требованиями настоящего стандарта.

3.2 Область применения и цели СМПИ

Организация должна определить область применения и цели СМПИ с учетом:

a) требований к менеджменту персональной информации;

b) целей и обязательств высшего руководства организации;

c) уровня приемлемого риска организации;

d) законодательных, обязательных, договорных и/или профессиональных требований;

e) интересов физических лиц и ключевых заинтересованных сторон.

3.3 Политика в области персональной информации

Высшее руководство организации должно официально сформулировать и нести ответственность за разработку и актуализацию политики организации в области персональной информации, обеспечить основу для соблюдения законодательных и обязательных требований и соответствие передовому опыту в области защиты данных.

Примечание - Высшее руководство обычно включает в себя совет директоров, генерального директора и руководителей высшего звена организации и/или владельца индивидуального предприятия.

В политике должна быть определена область применения СМПИ:

a) ко всей организации;

b) к соответствующим подразделениям и уровням организации.

Политика менеджмента персональной информации должна быть доведена до сведения всего персонала организации.

3.4 Содержание политики

В политике должны быть определены обязательства высшего руководства организации по соблюдению законодательных и обязательных требований и соответствию передовому опыту в области защиты персональных данных, включая:

a) обработку персональной информации только в случаях, когда это необходимо для достижения целей организации;

b) отказ от обработки излишней персональной информации;

c) предоставление физическим лицам достоверной информации о том, как их персональная информация будет использована и кем;

d) обработку только необходимой и адекватной персональной информации;

e) добросовестную и законную обработку персональной информации (см. п.4.7);

f) ведение реестра категорий персональной информации, обрабатываемой организацией (см. п.4.2);

g) обеспечение достоверности и, при необходимости, актуальности персональной информации;

h) хранение персональной информации в течение срока, установленного в соответствии с законодательными и обязательными требованиями для достижения установленных целей организации;

i) соблюдение прав лиц в отношении их персональной информации, включая их право на доступ к личным данным;

j) обеспечение защиты всей персональной информации;

k) трансграничную передачу персональной информации только при условии, что эта информация может быть должным образом защищена;

l) применение различных исключений, допустимых в соответствии с законодательством о защите персональных данных;

m) разработку и внедрение СМПИ с целью реализации политики;

n) если целесообразно, определение внутренних и внешних заинтересованных лиц и степени их участия в управлении СМПИ организации;

o) определение персональной ответственности уполномоченного персонала за менеджмент персональной информации организации (см. п.3.5).

3.5 Ответственность и подотчетность

Из числа высшего руководства должен быть назначен представитель, ответственный за менеджмент персональной информации в организации, который должен быть способен продемонстрировать соблюдение законодательных и обязательных требований и соответствие передовому опыту в области защиты персональных данных (см. п.4.1.1). Ответственный представитель должен нести ответственность за:

a) утверждение высшим руководством политики менеджмента персональной информации;

b) разработку и внедрение СМПИ в соответствие с политикой менеджмента персональной информации;

c) менеджмент безопасности и риска, направленный на выполнение политики менеджмента персональной информации (см. п.4.13.1).

Должны быть назначены лицо или группа лиц из числа персонала, обладающих соответствующей квалификацией и опытом, ответственными за каждодневное выполнение политики менеджмента персональной информации в организации (см. п.4.1.2).

В реализации политики менеджмента персональной информации должен участвовать весь персонал организации, выполняя процессы и процедуры организации. Это может быть достигнуто путем повышения квалификации работников, внедрением процедур по устранению несоответствий и применения соответствующих санкций.

3.6 Выделение ресурсов

Организация должна обеспечить необходимые ресурсы для создания, внедрения, функционирования и поддержания в рабочем состоянии СМПИ.

3.7 Внедрение СМПИ в организации

Для того, чтобы менеджмент персональной информации стал частью основных ценностей, активов и менеджмента, организация должна:

a) повышать и поддерживать осведомленность персонала о СМПИ путем организации постоянного обучения и выполнения программ повышения осведомленности персонала;

b) установить процесс оценки результативности в области повышения осведомленности о СМПИ;

c) информировать персонал о важности:

1) выполнения целей СМПИ;

2) соблюдения политики в области персональной информации;

3) постоянного улучшения политики в области персональной информации;

d) информировать персонал о его вкладе в достижение целей СМПИ организации и последствиях несоблюдения политики СМПИ.

4 Внедрение и функционирование СМПИ

4.1 Распределение ответственности и полномочий

Цель: Распределение ответственности и полномочий персонала в соответствии с политикой организации в области персональной информации.

4.1.1 Высшее руководство

Должен быть назначен представитель высшего руководства ответственный за менеджмент персональной информации в организации, который должен осуществляться таким образом, чтобы можно было продемонстрировать соблюдение законодательных и обязательных требований и соответствие передовому опыту в области защиты персональных данных

Примечание - В небольших организациях представитель высшего руководства и работник, ответственный за соблюдение политики (см. п.4.1.2), может быть одним и тем же лицом.

4.1.2 Ответственность за соблюдение политики

Один или несколько работников, обладающих соответствующей квалификацией и опытом работы, должны быть назначены ответственными за соблюдение политики менеджмента персональной информации организации. Возложенные обязанности могут выполняться на основе полной или частичной занятости в зависимости от размера организации и характера обработки персональной информации.

Назначенный персонал должен нести ответственность за:

a) соблюдение политики менеджмента персональной информации;

b) разработку и пересмотр политики менеджмента персональной информации;

c) обеспечение внедрения политики в области персональной информации;

d) анализ политики в области персональной информации со стороны высшего руководства (см. п.5.2);

e) обучение и постоянное повышение осведомленности персонала организации в соответствии с политикой в области персональной информации (см. п.4.3);

f) утверждение процедур, предусматривающих обработку персональной информации, таких как:

1) управление уведомлениями о конфиденциальности и обмен информацией о них (см. п.4.7.1);

2) работу с запросами физических лиц (см. п.4.12.1);

3) сбор и обработку персональной информации (см. п.4.7.1);

4) работу с претензиями (см. п.4.12.2);

5) устранение инцидентов в области безопасности (см. п.4.13.6);

6) аутсорсинг и передачу персональных данных в другие организации (см. п.4.14).

g) связь с лицами, ответственными за менеджмент риска и безопасности в организации (см. п.4.13);

h) предоставление консультаций и рекомендаций экспертов по вопросам защиты персональных данных;

i) интерпретацию и применение различных исключений при обработке персональной информации (см. введение и п.4.8.1);

j) предоставление рекомендаций по проектам, связанным с обменом данными (включая вопросы безопасности в ситуации, когда данные находятся вне зоны контроля) (см. п.4.8.3);

k) обеспечение доступа организации к актуализированным законодательным требованиям и рекомендациям о защите персональных данных (см. п.4.5);

l) мониторинг изменений в законодательстве, методах и технологиях в области защиты информации в СМПИ (см. п.4.5);

m) оформление, передачу и управление уведомлениями в адрес уполномоченного органа по защите прав субъектов персональных данных (далее - уполномоченный орган), если это требуется согласно закону о защите персональных данных (см. п.4.6);

n) внедрение методов, связанных с обработкой персональной информации, установленных в стандартах и/или рекомендациях.

4.1.3 Уполномоченные представители по защите данных

Если в организации существуют несколько подразделений, занимающихся обработкой персональной информации, или систем по обработке информации, то организация должна создать сеть уполномоченных представителей по защите персональных данных, которые:

a) представляют подразделения или системы с высоким уровнем риска в отношении менеджмента персональной информации (в п.4.2.2 см. примеры персональной информации, входящие в категории высокого уровня риска);

b) помогают персоналу, ответственному за выполнение политики.

4.2 Идентификация и регистрация используемых персональных данных

Цель: Обеспечение понимания персоналом организации категорий обрабатываемой персональной информации и уровня риска, возникающего при ее обработке.

4.2.1 Общие положения

Организация должна вести реестр категорий обрабатываемой персональной информации. В реестре должны быть указаны цели использования каждой категории персональной информации.

Примечание - Реестр должен обеспечивать все необходимые данные для уведомления уполномоченного органа об обработке персональных данных.

Организация должна отслеживать и документально оформлять прохождение персональной информации в рамках действующих процессов организации.

4.2.2 Персональная информация с высоким уровнем риска

Порядок ведения реестра (см. п.4.2.1) должен обеспечивать идентификацию и регистрацию категории обрабатываемой персональной информации с высоким уровнем риска.

Категории персональной информации с высоким уровнем риска могут включать в себя:

a) персональную информацию особой ответственности;

b) информацию о лицевых банковских счетах и другую финансовую информацию;

c) идентификаторы национальных систем, такие как номер страхового пенсионного полиса;

d) персональную информацию, касающуюся социально уязвимых взрослых и детей;

e) подробные профили данных физических лиц;

f) данные конфиденциальных переговоров, которые могут неблагоприятно повлиять на состояние и положение физического лица.

Примечание - Уровень риска может повышаться при обработке больших объемов персональной информации.

4.3 Обучение и осведомленность

Цель: Обеспечение осведомленности всего персонала организации о своих обязанностях, связанных с обработкой персональной информации.

Организация должна обеспечить, чтобы персонал, ответственный за соблюдение законодательных и обязательных требований и соответствие организации передовому опыту в области защиты персональных данных (см. п.4.1.2), был способен продемонстрировать свою компетентность в данной области, в том числе понимание требований и реализации СМПИ в организации. Организация также должна обеспечить осведомленность каждого работника в вопросах, связанных с менеджментом персональной информации, например, путем проведения обучения или обеспечения соответствующей информацией.

Организация должна быть в состоянии продемонстрировать понимание всем персоналом своей ответственности за защиту и обработку персональной информации в соответствии с установленными процедурами и требованиями безопасности.

Весь персонал организации должен пройти обучение методам обработки персональной информации в соответствии с установленными документированными процедурами организации. Обучение должно соответствовать функциям, обязанностям и полномочиям работника в организации.

4.4 Оценка риска

Цель: Обеспечение осведомленности организации обо всех видах риска, связанных с

обработкой конкретных видов персональной информации.

Организация должна внедрить процесс оценки риска для физических лиц, связанного с обработкой их персональной информации. Такая оценка также должна включать обработку персональных данных, осуществляемую другими организациями. Организация должна управлять риском, выявленным в процессе его оценки риска для снижения вероятности несоблюдения политики в области защиты персональной информации.

Процесс оценки риска должен включать в себя процедуры, в соответствие с которыми риск нанесения ущерба и/или причинения вреда физическим лицам при обработке персональной информации должен быть передан для анализа ответственным за защиту информации лицам и учтен (см. п.3.5) в системе менеджмента персональной информации.

Примечание - Организация может использовать различные методы оценки риска, например установленные ГОСТ Р ИСО/МЭК 31010. Кроме того, могут быть использованы иные нормативные документы, связанные с оценкой воздействия нарушения личной тайны.

4.5 Поддержка СМПИ

Цель: Оценка соответствия СМПИ для поддержки и постоянного улучшения соблюдения законодательных и обязательных требований и соответствия передовому опыту в области защиты персональных данных.

Персонал, ответственный за выполнение политики (см. п.4.1.2), должен постоянно оценивать способность СМПИ демонстрировать соблюдение законодательных и обязательных требований и соответствие передовому опыту в области защиты персональных данных.

Данная оценка должна включать в себя пересмотр СМПИ при изменении требований и/или методов работы организации.

4.6 Уведомление

Цель: Обеспечение необходимой отчетности организацией об обработке персональной информации перед уполномоченным органом в соответствии с требованиями [1].

СМПИ должна включать в себя процедуры уведомления уполномоченного органа (если организация не освобождена от требования подавать уведомления согласно [1]), а также должна обеспечивать точность и актуальность таких уведомлений.

4.7 Добросовестная и законная обработка информации

Цель: Обеспечение квалифицированной обработки персональной информации и установления законных оснований для обработки персональной информации до начала ее обработки.

4.7.1 Сбор и обработка персональной информации

СМПИ должна включать в себя процедуры, обеспечивающие:

a) квалифицированную и законную обработку персональной информации организацией;

b) обработку организацией персональной информации особой ответственности только в соответствии с требованиями [1];

c) обработку организацией персональной информации особой ответственности только для достижения установленных целей организации и в соответствии с требованиями [1];

d) выдачу лицу, передающему организации свою персональную информацию, "уведомления о конфиденциальности" или заявления о конфиденциальности в режиме он-лайн, полностью или частично со ссылкой на полный текст уведомления с указанием следующей информации:

1) сведений об организации;

2) цели обработки персональной информации;

3) условиях раскрытия персональных данных третьим лицам;

4) правах доступа субъекта к своим персональным данным;

5) условиях передачи персональной информации в страны, не обеспечивающие ее адекватной защиты;

6) способах обращения с запросом об обработке персональной информации в организации;

7) методах и технологиях, таких как файлы cookie, используемых на веб-сайте для сбора персональной информации о физических лицах;

8) прочих способах обеспечения квалифицированной обработки персональных данных.

Если сбор или использование персональной информации осуществляется для целей маркетинга, СМПИ должна включать в себя процедуры, обеспечивающие способы отказа субъекта персональных данных от подобного маркетинга, которые должны быть однозначно ему разъяснены.

СМПИ должна включать в себя процедуры, обеспечивающие порядок работы в ситуации, когда обработка персональных данных была основана на согласии субъекта персональной информации, которое позднее было им отозвано, т.е. процедуры прекращения обработки.

Если в соответствии с законодательными или обязательными требованиями необходимо согласие для осуществления маркетинга, СМПИ должна включать в себя процедуры получения такого согласия.

Если персональную информацию особой ответственности получают для определенных целей, СМПИ должна включать в себя процедуры, обеспечивающие точное указание в уведомлениях о конфиденциальности целей использования такой персональной информации.

СМПИ должна включать в себя процедуры, обеспечивающие верификацию и валидацию новых методов сбора информации персоналом, обладающим соответствующей квалификацией и опытом работы (см. п.4.1.2), и соответствие таких методов законодательным и обязательным требованиям и передовому опыту в области защиты персональных данных.

4.7.2 Записи об уведомлениях и заявлениях о конфиденциальности

СМПИ должна включать в себя процедуры регистрации уведомлений и он-лайн заявлений о конфиденциальности. Такие записи должны храниться не менее установленного срока хранения соответствующей персональной информации.

4.7.3 Срок предоставления уведомлений и заявлений о конфиденциальности

СМПИ должна включать в себя процедуры, обеспечивающие порядок действий в ситуации, когда организация получает персональную информацию непосредственно от физического лица, при этом уведомление или он-лайн заявление о конфиденциальности должно быть предоставлено или доступно этому лицу до получения от него какой-либо персональной информации.

4.7.4 Доступность уведомлений и заявлений о конфиденциальности

СМПИ должна включать в себя процедуры, обеспечивающие понятность и доступность содержания всех уведомлений и/или он-лайн заявлений о конфиденциальности.

Примечание - Уведомления о конфиденциальности, используемые при сборе персональной информации у социально уязвимых взрослых лиц и детей, а также лиц, испытывающих затруднения в обучении, должны быть представлены на языке и в формате,понятном и доступном для них.

4.7.5 Третьи стороны

СМПИ должна включать в себя процедуры, обеспечивающие добросовестность и законность получения персональной информации от третьих сторон.

СМПИ должна включать в себя процедуры, обеспечивающие, при необходимости, предоставление субъектам персональной информации уведомлений о конфиденциальности и/ онлайн заявление о конфиденциальности (см. п.4.7.1), за исключением случаев, когда такие меры являются чрезмерными.

Примечание - Предоставление уведомления или онлайн заявления о конфиденциальности могут быть признаны "чрезмерной мерой", если для этого организации требуются "значительные усилия" или если обработка информации может с большой вероятностью нанести ущерб субъекту.

4.8 Обработка персональных данных в заявленных целях

Цель: Обеспечение сбора и обработки персональной информации только для достижения установленных и заявленных целей.

4.8.1 Основания для обработки персональной информации

СМПИ должна включать процедуры, обеспечивающие при обработке персональной информации соблюдение законодательных требований, нормативных актов или контрактных обязательств.

СМПИ должна включать процедуры, не допускающие использование собранной для конкретных целей персональной информации в иных целях, за исключением случаев, когда:

a) применимо соответствующее исключение из закона;

b) имеется дополнительное согласие лиц на обработку их персональной информации в иных целях.

СМПИ должна включать в себя процедуры, обеспечивающие получение согласия лица на обработку его персональной информации особой ответственности для новых целей до начала этой обработки, кроме ситуаций, когда применимо соответствующее исключение из законодательных требований.

4.8.2 Согласие на обработку персональной информации для новых целей

СМПИ должна включать в себя процедуры, обеспечивающие получение добровольного и осознанного согласия на обработку персональной информации для новых целей. СМПИ должна включать в себя процедуры, обеспечивающие:

a) получение однозначного подтверждения согласия лица на использование его персональной информации для новых целей;

b) регистрацию полученных согласий на обработку персональной информации для новых целей.

4.8.3 Обмен данными

СМПИ должна включать в себя процедуры, обеспечивающие формальное установление ответственности относительно персональной информации в письменном соглашении или договорах в ситуации, когда организация передает персональную информацию другой организации.

СМПИ должна включать в себя процедуры, устанавливающие требования к использованию персональной информации другими организациями в своих целях. Для этого:

a) письменное соглашение или договор должны установить цели использования информации и ограничения на дальнейшее использование персональной информации в иных целях;

b) другая организация должна предоставить заявление или иное доказательство взятого на себя обязательства обрабатывать информацию в соответствии с требованиями [1].

СМПИ должна включать в себя процедуры, устанавливающие требования к новым видам обработки персональной информации, включая обмен данными с третьими лицами только при уведомлении организации (см. п.4.6) и в соответствии с условиями уведомления о конфиденциальности или он-лайн заявления о конфиденциальности [см. п.4.7.1 d)], предоставленного субъекту персональных данных. В противном случае организация должна обеспечивать наличие:

1) законных оснований для обмена данными;

2) согласие лица на обмен данными, при необходимости.

Если обмен данными с третьими лицами разрешен без согласия субъекта персональных данных, СМПИ должна включать в себя процедуры, обеспечивающие ведение и регулярный анализ протоколов обмена данными и наличие документированных процедур и методов контроля обмена данными.

Если требуется обмен данными с третьими лицами, например, в соответствие с законодательными требованиями, СМПИ должна включать в себя процедуры, обеспечивающие наличие протоколов и методов контроля обмена данными.

4.8.4 Объединение данных

Если персональная информация объединяется с другой персональной информацией для создания, например, расширенного профиля идентифицируемого субъекта персональных данных, СМПИ должна включать в себя процедуры, обеспечивающие использование объединенной персональной информация исключительно для достижения заявленных и совместимых с ними целей, в соответствии с полученным согласием субъекта и законодательными требованиями.

4.9 Адекватность, соответствие целям и достаточность

Цель: Организация должна обеспечить адекватность, соответствие целям обработки и достаточность персональной информации.

4.9.1 Адекватность

СМПИ должна включать в себя процедуры, обеспечивающие сбор персональной информации, адекватной целям организации.

СМПИ должна включать в себя процедуры актуализации методов и процессов обработки персональной информации, обеспечивающих адекватность персональной информации этим целям.

4.9.2 Соответствие целям и неизбыточность

СМПИ должна включать процедуры, обеспечивающие следующее:

a) организация должна обрабатывать минимальное количество персональной информации, необходимой для достижения ее целей;

b) организация не должна обрабатывать дополнительную персональную информацию, которая является несоответствующей или излишней для целей организации, за исключением случаев, когда предоставление такой информации не является обязательным, и она обрабатывается с согласия субъекта персональной информации;

c) новые системы и процессы, включающие обработку персональной информации, следует анализировать для обеспечения соответствия обрабатываемой информации целям ее обработки и достаточности.

Если для достижения целей организации нет необходимости или нецелесообразно обрабатывать персональную информацию, СМПИ должна регламентировать условия, при которых обработка персональной информации не производится.

4.10 Достоверность

Цель: Обеспечение достоверности персональной информации и, при необходимости, ее актуализация.

СМПИ должна включать в себя процедуры, обеспечивающие целостность и достоверность обрабатываемой персональной информации.

СМПИ должна включать в себя процедуры, позволяющие физическим лицам оспаривать достоверность их персональной информации и, при необходимости, вносить в нее исправления. Если персональная информация является недостоверной и не подлежит исправлению, например, в отношении исторических данных, СМПИ должна включать процедуры регистрации обнаруженных недостоверных данных и, если это правомерно, соответствующей достоверной персональной информации.

СМПИ должна включать в себя процедуры проверки выявленных случаев недостоверности данных.

СМПИ должна включать в себя процедуры, обеспечивающие информирование персонала о важности точной записи персональной информации и об использовании только актуальной персональной информации при принятии важных решений в отношении физических лиц.

СМПИ должна включать в себя процедуры:

a) информирования третьих сторон, которым организация передала недостоверную или устаревшую персональную информацию, о том, что информация является недостоверной и (или) устаревшей и не должна использоваться при принятии решений в отношении субъектов персональной информации;

b) передачи исправленной персональной информации третьим сторонам, при необходимости.

СМПИ должна включать в себя процедуры проверки новых систем и процессов, включающих обработку персональной информации и обеспечивающих:

1) подтверждение, что новые системы или процессы способны предупредить запись недостоверной или устаревшей персональной информации;

2) внесение изменений в недостоверную или устаревшую персональную информацию.

4.11 Хранение и уничтожение

Цель: Обеспечение хранения персональной информации в течение установленного срока.

В СМПИ должен быть установлен порядок хранения персональной информации, включая:

a) минимальные сроки хранения, установленные в соответствие с законодательными и/или обязательными требованиями;

b) определения и обоснования основных принципов назначения сроков хранения персональной информации;

c) обоснование хранения персональной информации в течение срока, превышающего установленный период хранения, например, для статистических и (или) исследовательских целей.

СМПИ должна включать в себя процедуры внедрения порядка (план-графика) хранения и доведения его до сведения исполнителей.

СМПИ должна включать в себя процедуры уничтожение персональной информации, которая больше не требуется организации.

СМПИ должна включать в себя процедуры уничтожения или ссылку на них, включая:

1) использование утвержденных процедур;

2) обеспечение уровня безопасности, соответствующего важности и чувствительности персональной информации;

3) управление персональной информацией в соответствии с оценкой риска информационной безопасности организации.

Примечание - Иногда целесообразно передать персональную информацию на постоянное хранение в архив.

4.12 Права субъектов персональных данных

Цель: Обеспечение в существующих процедурах соблюдения прав субъектов персональных данных.

4.12.1 Соблюдение прав субъектов персональных данных

СМПИ должна включать процедуры, обеспечивающие соблюдение прав физических лиц в отношении их персональной информации и обработку в короткие сроки, установленные законом, запросов на использование таких прав.

Примечание - Эти права включают в себя доступ к информации, возможность отказа от ее обработки и проверку автоматизированной обработки.

4.12.2 Претензии и апелляции

СМПИ должна включать в себя процедуру работы с претензиями к обработке персональной информации. Должны быть также установлены процедуры рассмотрения апелляций физических лиц в отношении работы с их претензиями.

4.13 Обеспечение безопасности

Цель: Обеспечить защиту персональной информации от потери или повреждения и несанкционированной или незаконной обработки путем реализации соответствующих технических и организационных мер по обеспечению безопасности.

4.13.1 Способы обеспечения безопасности

СМПИ должна определить необходимые способы обеспечения безопасности, соответствующие:

a) категории обрабатываемой персональной информации;

b) риску причинения ущерба или моральных потерь лицам в случае появления компрометирующей информации (см. п.4.4).

Примечание 1 - Оценка риска (4.4) должна установить соответствующий уровень контроля и управление безопасностью. Чрезмерные требования безопасности могут быть не менее опасными, чем недостаточные требования.

При обработке персональной информации с высоким уровнем риска (см. п.4.2.2) СМПИ должна обеспечивать постоянное соответствие установленных и используемых мер безопасности уровню риска.

Примечание 2 - Часто для обеспечения соответствия требованиям безопасности целесообразно применение стандарта ГОСТ Р ИСО/МЭК 27001, возможна также оценка

соответствия требованиям этого стандарта внешним органом по оценке соответствия.

4.13.2 Хранение и обработка

СМПИ должна включать в себя процедуры, обеспечивающие безопасное хранение и обработку персональной информации в соответствии с уровнем ее конфиденциальности и особой ответственности.

Примечание - Особое внимание следует обратить на хранение персональной информации на носителях и портативных устройствах, таких как ленточные накопители для резервного копирования, переносные накопители USB, съемные жесткие диски, ноутбуки и другие устройства.

4.13.3 Передача

СМПИ должна включать в себя процедуры, обеспечивающие передачу персональной информации в электронном виде и/или вручную внутри организации, и/или в другие организации, ее защиту средствами, установленными организацией для защиты информации при передаче.

4.13.4 Методы управления доступом

СМПИ должна включать в себя процедуры, обеспечивающие доступ к персональной информации только сотрудникам, которым это необходимо для выполнения их должностных обязанностей.

СМПИ должна включать в себя процедуры, обеспечивающие при предоставлении законного доступа к персональной информации понимание персоналом того, что доступ предоставляется исключительно в служебных целях и должен осуществляться исключительно в законных основаниях.

При обработке персональной информации с высоким уровнем риска (см. п.4.2.2) СМПИ должна включать в себя процедуры, обеспечивающие способы управления и контроля доступа, которые должны быть взаимосвязаны с уровнем важности и чувствительности персональной информации.

СМПИ должна включать в себя процедуры, обеспечивающие контроль всех случаев доступа к персональной информации и их оценку в соответствии с процедурой оценки риска информационной безопасности организации.

4.13.5 Оценка безопасности

СМПИ должна включать в себя процедуры, обеспечивающие регулярное проведение оценки безопасности.

В результате оценки должны быть оценены адекватность существующих методов и

способов обеспечения безопасности и, при необходимости, даны рекомендации по их улучшению.

При проведении оценки необходимо учитывать риск причинения вреда, ущерба и (или) моральных потерь лицам в случае возникновения инцидента, связанного с безопасностью.

4.13.6 Управление инцидентами, связанными с безопасностью

СМПИ должна включать в себя процедуры:

a) оценки и управления инцидентами, связанными с безопасностью персональной информации, включая процедуры смягчения ущерба, причиненного этими инцидентами;

b) документирования каждого инцидента, связанного с безопасностью, включая оценку того, как он произошел, какие корректирующие действия были предприняты и какие выводы были сделаны;

c) принятия решений о необходимости направления сообщения об инциденте, связанном с безопасностью, соответствующему регулирующему органу или оповещения субъектов персональных данных;

d) регистрации таких сообщений и выданных оповещений.

4.14 Трансграничная передача персональных данных за пределы РФ

Цель: Обеспечить соответствующий уровень защиты при передаче или обработке персональной информации за пределами страны.

СМПИ должна включать в себя процедуры, обеспечивающие защиту прав физических лиц, если организация передает персональную информацию за пределы РФ, в том числе:

a) необходимо включить в договора условия, обеспечивающие защиту информации и процесса ее обработки, например, использование типовых договоров и/или установление внутренних обязательных требований к работе с персональной информацией для организаций, получающих информацию;

b) при передаче персональной информации в организации, находящиеся в других странах, следует установить соответствие этой организации международным требованиям обеспечения безопасности персональной информации;

c) установление страны местонахождения организации, которой передается персональная информация, и оценка этой страны на предмет обеспечения адекватной защиты этой информации;

d) если организация, получающая информацию, привлекает другие организации (субподрядчиков) к обработке персональной информации, следует провести проверку таких организаций.

СМПИ должна включать в себя процедуры, обеспечивающие анализ и проверку персоналом, ответственным за соблюдение законодательных и обязательных требований и соответствие передовому мировому опыту в области защиты персональных данных (см. п.4.1.2), всех новых предложений, включающих передачу персональной информации за пределы РФ. В результате такого анализа и проверки должны быть установлены возможности обеспечения адекватной защиты персональной информации при такой передаче.

СМПИ должна включать в себя процедуры, обеспечивающие наличие типовых договоров с субподрядчиками, которые обрабатывают персональную информацию от имени организации и расположены за пределами РФ. Такие типовые договора, необходимы для обеспечения надлежащей защиты персональной информации, если не согласованы иные адекватные процедуры защиты информации.

4.15 Раскрытие информации третьим сторонам

Цель: Организация должна обеспечить управление раскрытием информации третьим сторонам в соответствии с законодательными и обязательными требованиями и передовым опытом в области защиты данных.

СМПИ должна включать в себя процедуры, обеспечивающие предоставление третьими сторонами объективных свидетельств:

a) их права на доступ к персональной информации;

b) их подлинности, при необходимости.

СМПИ должна включать в себя процедуры, обеспечивающие проведение проверки наличия законных оснований для раскрытия информации третьим сторонам.

Третьим сторонам должен раскрываться только минимально необходимый объем персональной информации.

СМПИ должна включать в себя процедуры регистрации записей о фактах раскрытия персональной информации. Записи должны стать объективным свидетельством того, что раскрытие было законным и позволить организации контролировать раскрытие персональной информации.

Примечание - Если доступ к персональной информации предоставляется третьим сторонам на основании закона, то проверку подлинности и минимизации объема раскрываемой информации можно не проводить.

4.16 Передача обработки информации при привлечении субподрядчиков

Цель: Организация должна обеспечить, чтобы обработка персональной информации, обрабатываемой подрядчиком от имени организации, осуществлялась в соответствии с законодательными и обязательными требованиями и передовым опытом в области защиты данных.

Если обработка персональной информации от имени организации проводится подрядчиком, СМПИ должна включать в себя процедуры, обеспечивающие:

a) выбор организацией подрядчиков, способных обеспечить техническую, физическую и организационную безопасность в соответствии с требованиями организации в отношении персональной информации;

b) проведение организацией тщательной проверки выбранного подрядчика, оценки соответствующих мер безопасности в области защиты данных и, при необходимости, проверки мер безопасности, применяемых подрядчиком до заключения договора в зависимости от характера обрабатываемой персональной информации или обстоятельств, сопутствующих ее обработке;

c) составление договора об оказании услуг в письменной форме, требующего от выбранного подрядчика обеспечения надлежащего уровня безопасности обрабатываемой персональной информации;

d) проведение регулярных проверок мер безопасности у подрядчика в течение всего срока его доступа к персональной информации;

e) выполнение подрядчиком обязательств по получению от организации разрешения на использование услуг субподрядчиков для обработки персональной информации в соответствии с договором;

f) включение в договор субподряда требования к субподрядчику (и это требование распространяется далее и на его субподрядчиков) о соблюдении, как минимум, таких же требований по безопасности и других положений, которые применимы к подрядчику;

g) установления в договорах подряда (которые передаются и субподрядчикам) требования уничтожения соответствующей персональной информации либо передаче ее организации или подрядчику (по указанию организации) при прекращении действия договора.

4.17 Поддержка

СМПИ должна включать в себя процедуры, обеспечивающие актуализацию процедур и элементов обработки информации для поддержания их корректного и надлежащего функционирования. Такие процедуры должны обеспечивать регулярное планирование и проведение мероприятий по поддержке СМПИ.

5 Мониторинг и анализ СМПИ

Цель: Обеспечение мониторинга и анализ результативности и эффективности СМПИ.

5.1 Внутренний аудит

5.1.1 Планирование аудита

Планирование, установление и поддержка программы аудита по мониторингу и анализу результативности и эффективности обработки организацией персональной информации должны проводиться с учетом политики в области персональной информации.

Программа аудита должна включать в себя проверку всех элементов обработки персональной информации, а также информации с высоким уровнем риска (см. п.4.2.2) и обработки персональной информации подрядчиками (см. п.4.16).

5.1.2 Выбор аудиторов

Объективность и независимость аудита должны быть основаны на правильном выборе аудиторов и управлении программами аудита.

Примечание - Для крупных организаций и организаций, обрабатывающих персональную информацию с высоким уровнем риска (см. пункт 4.2.2), следует рассмотреть варианты проведения регулярного внешнего аудита.

5.1.3 Требования к аудиту

Аудит должен проводиться через запланированные интервалы времени и предусматривать проверку:

a) функционирования СМПИ в соответствии с политикой и установленными процедурами;

b) внедрения и функционирования СМПИ в соответствии с технологическими требованиями.

Отчеты об аудите должны быть представлены руководству организации, в котором должны быть указаны все значимые отклонения от политики и (или) установленных процедур.

В отчетах об аудите должны быть идентифицированы вопросы, связанные с методами или процессами, которые могут повлиять на соблюдение политики в области персональной информации.

5.2 Анализ со стороны руководства

Анализ СМПИ со стороны руководства должен проводиться регулярно, а также в случае существенных изменений для обеспечения устойчивого развития, адекватности и эффективности системы.

Анализ со стороны руководства должен включать следующую информацию:

a) обратную связь, полученную от потребителей СМПИ;

b) идентификации персоналом опасных событий и их эскалации;

c) результатах аудита;

d) записях анализа процедур;

e) результатах модернизации и (или) замены технологий;

f) формальных запросах об оценке регулирующими органами;

g) обработке претензий;

h) случаях нарушений/инцидентов безопасности.

Анализ со стороны руководства должен представлять подробную информацию в отношении возможных изменений СМПИ, например, путем идентификации изменений в политике, процедурах и (или) методах, которые могут повлиять на обеспечение соответствия.

После внесения существенных изменений в СМПИ аудит должен проводиться в кратчайшие сроки.

6 Улучшение СМПИ

Цель: Организация должна улучшать результативность и эффективность СМПИ путем выполнения корректирующих и предупреждающих действий.

6.1 Предупреждающие и корректирующие действия

6.1.1 Общие положения

Организация должна постоянно улучшать СМПИ путем реализации предупреждающих и корректирующих действий.

Все предлагаемые изменения и/или улучшения должны быть оценены до начала их внедрения, чтобы обеспечить выполнение требований политики менеджмента персональной информации.

Изменения, которые могут негативно повлиять на возможность демонстрировать соблюдение законодательных и обязательных требований и передового опыта в области защиты данных (например, перевод персональной информации в новый формат хранения файлов), необходимо анализировать с целью определения их влияния на обеспечение соответствия.

Изменения, возникающие в результате реализации предупреждающих и корректирующих действий, следует документировать и обеспечить хранение данных в соответствии с их правилами хранения.

6.1.2 Предупреждающие действия

Организация должна принимать меры для защиты от потенциальных несоответствий для предотвращения их повторного появления. Должны быть установлены процедуры:

a) выявления несоответствий и их причин;

b) определения и реализации необходимых предупреждающих действий;

c) регистрации результатов анализа предпринятого действия;

d) идентификации изменившегося риска;

e) обеспечения информирования всех заинтересованных сторон о потенциальном несоответствии и предпринятом предупреждающем действии.

6.1.3 Корректирующие действия

В СМПИ должна быть установлена процедура анализа каждого несоответствия и, на основе оценки риска, выполнения следующих действий:

a) устранения причины несоответствия;

b) уменьшения степени несоответствия;

c) если в результате оценки риска установлено, что уменьшение степени несоответствия невозможно или требует неадекватных затрат, эти выводы и их обоснование должны быть документированы.

Оценку риска следует проводить регулярно с целью выявления изменений существующего положения и необходимости устранения несоответствий (см. п.4.4).

Организация должна обеспечить оценку всех вновь выявленных видов риска для персональной информации (внутри организации или в более широкой сфере) с использованием проактивных процедур, таких как оценка влияния нарушений конфиденциальности персональной информации.

6.2 Постоянное улучшение

Организация должна постоянно повышать результативность СМПИ, используя результаты аудита, предупреждающие и корректирующие действия и анализ со стороны руководства.

Претензии, инциденты безопасности, запросы на доступ к информации и прочие материалы следует использовать для улучшения эффективности СМПИ.

Приложение А (справочное). Цикл PDCA "Планирование - Осуществление - Проверка - Действие"

Приложение А
(справочное)

В настоящем стандарте применен цикл PDCA "Планирование-Осуществление-Проверка-Действие" для установления, внедрения, функционирования, мониторинга, использования, поддержания в рабочем состоянии и повышения эффективности СМПИ

организации. Он обеспечивает надлежащую степень соответствия другим стандартам системы менеджмента, таким образом, поддерживая последовательное и интегрированное внедрение и совместное функционирование с соответствующими системами менеджмента.

Другие стандарты систем менеджмента:

ГОСТ Р ИСО 9001 (Системы менеджмента качества);

ГОСТ Р ИСО 14001 (Системы экологического менеджмента);

ГОСТ Р ИСО/МЭК 27001 (Системы управления информационной безопасностью);

ГОСТ Р ИСО/МЭК 20000 (Управление ИТ-сервисами).

На рисунке А.1 показано функционирование СМПИ на основе требований настоящего стандарта.

Рисунок А.1 - Цикл PDCA применительно к менеджменту персональной информации

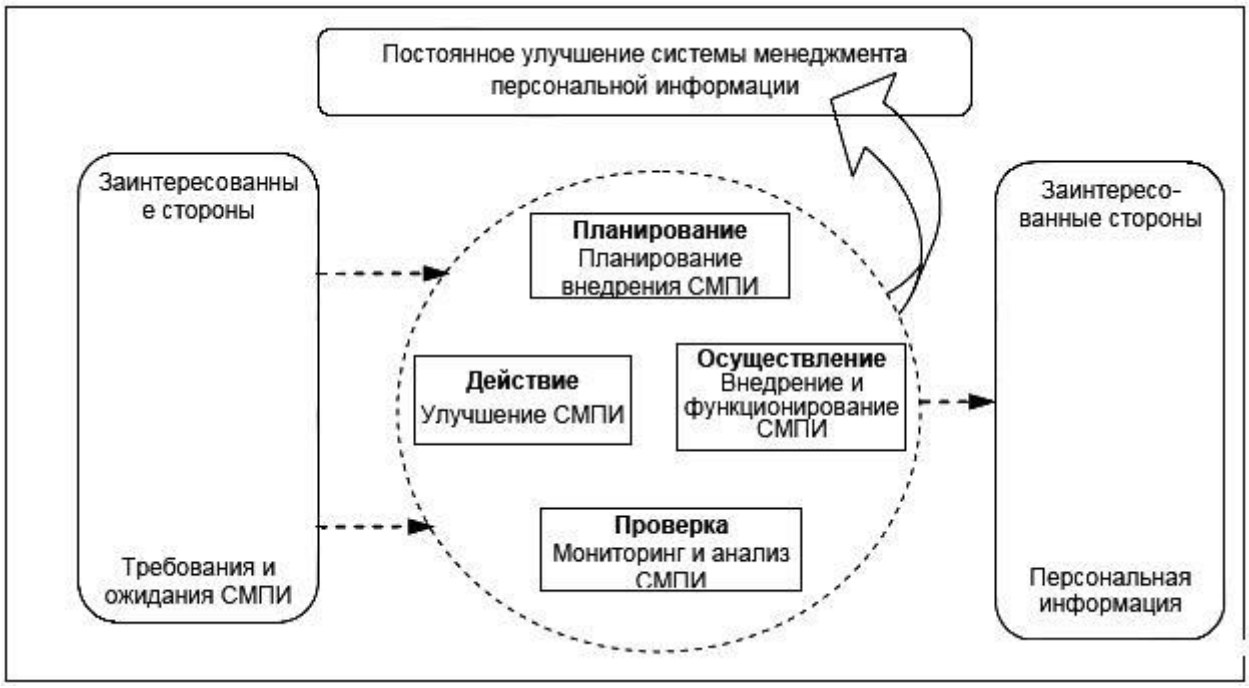

Рисунок А.1 - Цикл PDCA применительно к менеджменту персональной информации

Планирование	Планирование внедрения СМПИ	Раздел 3
Осуществление	Внедрение и функционирование СМПИ	Раздел 4

Проверка	Мониторинг и анализ СМПИ	Раздел 5
Действие	Улучшение СМПИ	Раздел 6

Библиография

[1] Федеральный закон "О защите персональных данных" N 152 от 27.07.2006 г.

[2] PARLIAMENT AND COUNCIL OF THE EUROPEAN COMMUNITY. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJL 281, 23.11.1995, p.31-50 (ES, DA, DE, EL, EN, FR, IT, NL, PT, Fl, SV)

[3] ГОСТ Р ИСО 9000-2008 Системы менеджмента качества. Основные положения и словарь

[4] ГОСТ Р ИСО 9001-2008 Системы менеджмента качества. Требования

[5] ГОСТ Р ИСО 14001-2007 Системы экологического менеджмента. Требования и руководство по применению

[6] ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

[7] ГОСТ Р ИСО/МЭК 20000-2-2010 Информационная технология. Менеджмент услуг. Часть 2. Кодекс практической деятельности

УДК 658:562.014:006.354 ОКС 03.100.01

Ключевые слова: защита данных, принципы защиты данных, персональные данные, менеджмент информации, менеджмент персональных данных, система менеджмента персональной информации, персональная информация особой ответственности.

Электронный текст документа
подготовлен АО "Кодекс" и сверен по:
официальное издание
М.: Стандартинформ, 2014