Международный союз электросвязи

МСЭ-Т X.1058

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(03/2017)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность информации и сетей – Управление безопасностью

Информационные технологии – Методы обеспечения безопасности – Свод правил и норм для защиты информации, позволяющей установить личность

Рекомендация МСЭ-Т X.1058

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	**X.1050–X.1069**
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
Рекомендации, связанные с PKI	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1379
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

МЕЖДУНАРОДНЫЙ СТАНДАРТ ISO/IEC 29151
Рекомендация МСЭ-Т X.1058

Информационные технологии – Методы обеспечения безопасности – Свод правил и норм для защиты информации, позволяющей установить личность

Резюме

Все больше организаций работают с информацией, позволяющей установить личность (PII), и все больше такой информации поступает в их распоряжение. Одновременно повышаются требования общества к защите PII и обеспечению безопасности данных о частных лицах. В ряде стран принимаются поправки и дополнения к законодательству в связи с участившимися случаями масштабной утечки данных.

В настоящей Спецификации устанавливаются задачи управления, средства управления для решения данных задач исходя из требований, выработанных по результатам оценки риска и анализа последствий для защиты PII, а также руководящие указания по реализации этих средств управления. В частности, настоящая Спецификация содержит руководящие указания на базе стандарта ИСО/МЭК 27002 с учетом требований к обработке PII, которые могут быть применимы в контексте свойственной организации среды рисков нарушения информационной безопасности.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1058	30.03.2017 г.	17-я	11.1002/1000/13182

Ключевые слова

Свод норм и правил; средство управления; руководящие указания по реализации; PII.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

		Стр.
1	Сфера применения	1
2	Нормативно-справочные документы	1
3	Определения и сокращения	1
3.1	Определения	1
3.2	Сокращения	2
4	Обзор	2
4.1	Задача защиты PII	2
4.2	Требования к защите PII	2
4.3	Средства управления	3
4.4	Выбор средств управления	3
4.5	Разработка руководящих указаний для конкретной организации	3
4.6	Соображения, касающиеся жизненного цикла	4
4.7	Структура настоящей Спецификации	4
5	Политика информационной безопасности	4
5.1	Руководящие указания по обеспечению информационной безопасности	4
6	Организация обеспечения информационной безопасности	5
6.1	Внутренняя организация	5
6.2	Мобильные устройства и телеработа	7
7	Безопасность кадровых ресурсов	7
7.1	Перед приемом на работу	7
7.2	В период работы по найму	7
7.3	Увольнение и перемещение на места работы	8
8	Управление активами	8
8.1	Ответственность за активы	8
8.2	Классификация информации	9
8.3	Обращение с носителями данных	10
9	Управление доступом	11
9.1	Бизнес-требования к управлению доступом	11
9.2	Управление доступом пользователей	11
9.3	Сфера ответственности пользователей	12
9.4	Управление доступом к системам и приложениям	12
10	Шифрование	13
10.1	Средства управления, связанные с шифрованием	13
11	Физическая безопасность и безопасность окружающей среды	14
11.1	Защищенные зоны	14
11.2	Оборудование	14
12	Эксплуатационная безопасность	15
12.1	Эксплуатационные процедуры и сферы ответственности	15
12.2	Защита от вредоносного программного обеспечения	16
12.3	Резервное копирование	16

Стр.

12.4 Ведение журнала и мониторинг ... 16
12.5 Управление системным программным обеспечением ... 17
12.6 Управление техническими уязвимостями ... 17
12.7 Соображения, касающиеся аудита информационных систем ... 18
13 Безопасность связи ... 18
13.1 Управление безопасностью сетей ... 18
13.2 Передача информации ... 18
14 Приобретение, развитие и техническое обслуживание информационных систем ... 19
14.1 Требования к безопасности информационных систем ... 19
14.2 Обеспечение безопасности в процессах развития и технической поддержки ... 19
14.3 Тестовые данные ... 20
15 Взаимоотношения с поставщиками ... 20
15.1 Информационная безопасность во взаимоотношениях с поставщиками ... 20
15.2 Управление оказанием услуг, предоставляемых поставщиками ... 22
16 Управление инцидентами в области информационной безопасности ... 22
16.1 Управление инцидентами в области информационной безопасности и повышением информационной безопасности ... 22
17 Аспекты информационной безопасности как фактор управления для обеспечения непрерывности деятельности ... 24
17.1 Непрерывность обеспечения информационной безопасности ... 24
17.2 Избыточность ... 24
18 Соответствие требованиям ... 24
18.1 Соответствие законодательным и договорным требованиям ... 24
18.2 Анализ уровня информационной безопасности ... 25
Приложение A – Расширенный комплекс средств управления для защиты PII ... 27
A.1 Общее ... 27
A.2 Общая политика использования и защиты PII ... 27
A.3 Согласие и выбор ... 28
A.4 Правомерность и характеристики целей ... 30
A.5 Ограничение на сбор информации ... 32
A.6 Минимизация объема данных ... 32
A.7 Ограничение на использование, хранение и раскрытие информации ... 34
A.8 Точность и качество ... 37
A.9 Открытость, прозрачность и уведомление ... 38
A.10 Участие и доступ субъектов PII ... 40
A.11 Подотчетность ... 43
A.12 Информационная безопасность ... 46
A.13 Соответствие требованиям защиты конфиденциальности ... 47
Библиография ... 49

Введение

Все больше организаций работают с информацией, позволяющей установить личность (PII), и все больше такой информации поступает в их распоряжение. Одновременно повышаются требования общества к защите PII и обеспечению безопасности данных о частных лицах. В ряде стран принимаются поправки и дополнения к законодательству в связи с участившимися случаями масштабной утечки данных.

По мере роста количества утечек организациям, которые собирают или обрабатывают PII, потребуются руководящие указания о том, как в целях защиты PII снизить риски нарушения конфиденциальности и смягчить их последствия для организации и затронутых частных лиц. Такие руководящие указания приведены в настоящей Спецификации.

Настоящая Спецификация содержит указания диспетчерам PII о самых разнообразных средствах управления для обеспечения информационной безопасности и защиты PII, которые широко применяются в соответствующих организациях различного профиля. Остальные части семейства стандартов ИСО/МЭК, перечень которых приведен ниже, содержат руководящие указания или требования, относящиеся к другим сторонам комплексного процесса защиты PII.

- Стандарт ИСО/МЭК 27001 устанавливает процесс управления информационной безопасностью и относящиеся к нему требования. Этот документ может служить основой для защиты PII.
- Стандарт ИСО/МЭК 27002 содержит руководящие указания о внутриорганизационных стандартах и практических методах управления информационной безопасностью, включая указания по выбору, реализации и надлежащей работе соответствующих средств управления исходя из свойственных данной организации рисков среды для обеспечения информационной безопасности.
- Стандарт ИСО/МЭК 27009 устанавливает требования к применению стандарта ИСО/МЭК 27001 в любом конкретном секторе (сфере, области применения или рыночном сегменте). В нем разъясняется, как устанавливать дополнительные требования помимо изложенных в стандарте ИСО/МЭК 27001, уточнять требования стандарта ИСО/МЭК 27001 и включать средства управления или комплексы таких средств в дополнение к тем, которые указаны в Приложении А к стандарту ИСО/МЭК 27001.
- Стандарт ИСО/МЭК 27018 содержит руководящие указания для организаций – поставщиков облачных услуг, выступающих в роли обработчиков PII.
- Стандарт ИСО/МЭК 29134 содержит руководящие указания по выявлению, анализу и оценке рисков нарушения конфиденциальности, а стандарт ИСО/МЭК 27005 совместно с ИСО/МЭК 27001 устанавливают методологию выявления, анализа и оценки рисков для обеспечения безопасности.

По итогам анализа рисков следует разработать всестороннюю систему взаимоувязанных средств управления, которые должны быть адаптированы для ведения конкретных способов обработки PII.

Настоящая Спецификация состоит из двух частей – основная часть в составе разделов 1–18 и нормативное приложение. Эта структура отражает обычную практику разработки секторальных расширений стандарта ИСО/МЭК 27002.

Структура основной части настоящей Спецификации, включая заголовки разделов, воспроизводит структуру основной части стандарта ИСО/МЭК 27002. Во введении и разделах 1–4 даются общие сведения об использовании настоящей Спецификации. Заголовки разделов 5–18 соответствуют заголовкам в стандарте ИСО/МЭК 27002, отражая то обстоятельство, что настоящей Спецификации основана на руководящих указаниях ИСО/МЭК 27002 и в дополнение к нему устанавливает новые средства управления, относящиеся конкретно к защите PII. Многие средства управления, установленные стандартом ИСО/МЭК 27002, не требуют расширения с точки зрения диспетчеров PII. В ряде случаев однако необходимы дополнительные руководящие указания по реализации этих средств управления, и такие указания даются под соответствующим заголовком (и номером раздела) из стандарта ИСО/МЭК 27002.

Нормативное приложение устанавливает расширенный комплекс средств управления конкретно для защиты PII в дополнение к средствам управления, которые устанавливаются стандартом ИСО/МЭК 27002. Эти новые средства управления для защиты PII и руководящие указания по их реализации подразделяются

на 12 категорий, соответствующих политике обеспечения конфиденциальности и 11 принципам обеспечения конфиденциальности из стандарта ИСО/МЭК 29100:

- согласие и выбор;
- правомерность и характеристика цели;
- ограничение по сбору;
- минимизация объема данных;
- ограничение по использованию, хранению и раскрытию данных;
- точность и качество;
- открытость, прозрачность и уведомление;
- личное участие и доступ;
- подотчетность;
- информационная безопасность; и
- соблюдение требований защиты конфиденциальности.

Рисунок 1 иллюстрирует связь между настоящей Спецификацией и семейством стандартов ИСО/МЭК.

Рисунок 1 – Связь между настоящей Спецификацией и семейством стандартов ИСО/МЭК

Настоящая Спецификация содержит руководящие указания на основе стандарта ISO/IEC 27002, модифицированные с учетом особых требований к защите конфиденциальности, возникающих в связи с обработкой PII:

a) в различных доменах обработки, таких как:
   - облачные услуги общего пользования;
   - приложения социальных сетей;
   - подключенные к интернету устройства бытового назначения;
   - поиск, анализ;
   - сбор PII для рекламных и аналогичных целей;
   - программы анализа больших массивов данных;
   - обработка данных по трудоустройству;
   - управление предприятиями по торговле и оказанию услуг (планирование ресурсов предприятий, управление отношениями с клиентами);

b) в различных местах, таких как:

– на персональной вычислительной платформе, предоставленной частному лицу (например, смарт-карты, смартфоны и приложения для них, интеллектуальные измерительные приборы, носимые устройства и т. д.);
– в сетях передачи и сбора данных (например, в тех случаях, когда данные о местоположении мобильного телефона, которые могут в некоторых юрисдикциях классифицироваться как PII, генерируются в ходе нормальной сетевой обработки);
– в рамках собственной вычислительной инфраструктуры организации;
– на вычислительной платформе третьей стороны;

c) для характеристик сбора, таких как:
– однократный сбор данных (например, регистрация для получения некоторой услуги);
– текущий сбор данных (например, частый мониторинг показателей жизнедеятельности с помощью датчиков, расположенных на теле или вживленных в организм, многократный сбор данных с использованием бесконтактных платежных карт для оплаты товаров и услуг, эксплуатация систем сбора показаний интеллектуальных измерительных приборов и т. д.).

ПРИМЕЧАНИЕ. – В текущем порядке может собираться или предоставляться PII об особенностях поведения, местоположении и других видах PII. В таких случаях необходимо рассматривать возможность использования средств управления для защиты PII, которые позволяли бы управлять доступом и сбором информации на основе согласия, а также обеспечивали субъекту PII надлежащий контроль над этой деятельностью по доступу и сбору информации.

МЕЖДУНАРОДНЫЙ СТАНДАРТ
РЕКОМЕНДАЦИЯ МСЭ-Т

Информационные технологии – Методы обеспечения безопасности – Свод правил и норм для защиты информации, позволяющей установить личность

1 Сфера применения

Настоящая Рекомендация | Международный стандарт устанавливает задачи управления в области защиты информации, позволяющей установить личность (PII), средства управления для решения данных задач исходя из требований, выработанных по результатам оценки риска и анализа последствий, а также руководящие указания по реализации этих средств управления.

В частности, данный документ содержит руководящие указания на основе стандарта ISO/IEC 27002 с учетом требований к обработке PII, которые потенциально применимы исходя из свойственных той или иной организации среды рисков для обеспечения информационной безопасности.

Настоящая Рекомендация | Международный стандарт применима к организациям всех типов и размеров, выступающим в роли диспетчеров PII (согласно определению в стандарте ISO/IEC 29100), включая частные и государственные компании, правительственные структуры и некоммерческие организации, обрабатывающие PII.

2 Нормативно-справочные документы

Нижеследующие Рекомендации и международные стандарты содержат положения, которые путем ссылки на них в данном тексте образуют положения настоящей Рекомендации | международного стандарта. На момент публикации указанные издания были действующими. Все Рекомендации и стандарты подвергаются пересмотру; поэтому всем сторонам соглашений, основанных на данной Рекомендации | международном стандарте, следует изучить возможность применения последнего издания перечисленных ниже Рекомендаций и стандартов. Члены МЭК и ИСО ведут реестры действующих в настоящее время международных стандартов. Бюро стандартизации электросвязи МСЭ ведет список действующих в настоящее время Рекомендаций МСЭ-Т.

- ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*
- ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls.*
- ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework.*

3 Определения и сокращения

3.1 Определения

Для целей настоящей Рекомендации | Международного стандарта используются термины и определения, приведенные в стандартах ISO/IEC 27000:2016 и ISO/IEC 29100, а также следующие термины и определения.

В стандартизации используются терминологические базы данных: *Онлайновая навигационная платформа ИСО*, Electropedia МЭК и *Термины и определения МСЭ*.

3.1.1 руководитель службы обеспечения конфиденциальности информации (chief privacy officer): руководящее лицо, которое несет ответственность за защиту информации, позволяющей установить личность (PII) в организации.

3.1.2 удаление идентификационной информации (de-identification): процесс удаления ассоциации между набором идентифицирующих данных и субъектом данных с помощью методов удаления идентификационной информации.

3.2 Сокращения

Для целей настоящей Спецификации используются следующие сокращения.

BCR	Binding Corporate Rules	Обязательные корпоративные правила
CCTV	Closed-Circuit Television	Система охранного видеонаблюдения
CPO	Chief Privacy Officer	Руководитель службы обеспечения конфиденциальности информации
PBD	Privacy by Design	Защита конфиденциальности на этапе проектирования
PDA	Personal Digital Assistants	Персональные цифровые помощники
PET	Privacy Enhancing Technology	Технология усиления защиты конфиденциальности
PIA	Privacy Impact Assessment	Оценка воздействия на защиту конфиденциальности
PII	Personally Identifiable Information	Информация, позволяющая установить личность
RFID	Radio Frequency Identification	Радиочастотная идентификация
USB	Universal Serial Bus	Универсальная последовательная шина

4 Обзор

4.1 Задача защиты PII

Настоящая Спецификация определяет комплекс средств управления для защиты PII. Цель защиты PII состоит в том, чтобы создать условия для внедрения организациями комплекса средств управления в рамках общей программы защиты PII. Этот комплекс может применяться для обеспечения и повышения уровня соответствия требованиям законов и регуляторных положений, управления рисками нарушения конфиденциальности, а также для оправдания ожиданий субъектов PII, регуляторных органов или клиентов в соответствии с принципами обеспечения защиты конфиденциальности, изложенными в стандарте ИСО/МЭК 29100.

4.2 Требования к защите PII

Организации следует определить свои требования к защите PII. Требования определяются в соответствии с принципами конфиденциальности, изложенными в стандарте ИСО/МЭК 29100. Существует три основных источника требований к защите PII:

- нормативно-правовые и договорные требования – в том числе, например, требования к защите PII, которые обязаны соблюдать сама организация, ее деловые партнеры, подрядчики и поставщики услуг;
- результаты оценки рисков (а именно рисков для безопасности и защиты конфиденциальности) организации и субъекта PII с учетом общих целей и стратегии деятельности организации;
- корпоративная политика, в рамках которой организация может добровольно выйти за пределы критериев, определяемых из перечисленных выше требований.

Кроме того, организациям следует учитывать принципы (то есть принципы конфиденциальности, изложенные в стандарте ИСО/МЭК 29100) и задачи обработки PII, а также бизнес-требования к обработке PII, разработанные в поддержку операционной деятельности организации.

Средства управления для защиты PII, в том числе средства управления безопасностью, следует выбирать по итогам оценки рисков. Результаты оценки воздействия на защиту конфиденциальности (PIA), проведенной, например, в соответствии со стандартом ИСО/МЭК 29134, помогут руководить процессом и определить надлежащий подход к управлению рисками для защиты PII и реализации выбранных средств управления для противодействия этим рискам, а также расставить соответствующие приоритеты.

За основу руководящих указаний по PIA (включая советы по проведению такой оценки, составлению плана противодействия рискам, принятию и пересмотру рисков) можно взять одну из спецификаций PIA, например стандарт ИСО/МЭК 29134.

4.3 Средства управления

Оценка рисков для защиты конфиденциальности может помочь организациям выявить конкретные риски в этой сфере, возникающие в связи с незаконной обработкой информации или неправомерным ограничением прав субъектов PII, которых затрагивает соответствующая операция. Организациям следует определить и реализовать средства управления для противодействия выявленным по результатам оценки последствия рисков. Далее эти средства управления и способы противодействия следует задокументировать, лучше всего в отдельном реестре рисков. При некоторых видах обработки PII может оказаться целесообразной реализация конкретных средств управления, потребность в которых становится очевидной только по итогам тщательного анализа планируемой операции.

4.4 Выбор средств управления

Средства управления для защиты PII могут выбираться из числа рассматриваемых в настоящей Спецификации (в которую посредством ссылки включены средства управления из стандарта ИСО/МЭК 27002, результатом чего является комбинированный типовой комплекс таких средств). При необходимости можно также выбирать средства управления из других наборов таких средств или разрабатывать новые средства управления, ориентированные на конкретные нужды.

Выбор средств управления определяется организационными решениями, принятыми исходя из критериев выбора способов противодействия рискам и общего подхода к управлению рисками применительно к самой организации и, через посредство договорных соглашений, к ее клиентам и поставщикам, а также должен отвечать требованиям всех соответствующих национальных и международных нормативно-правовых актов.

Кроме того, выбор и реализация средств управления зависят от роли данной организации в деятельности по предоставлению инфраструктуры или оказанию услуг. В такой деятельности может принимать участие множество организаций, причем в одних случаях выбранные средства управления могут быть делом конкретной организации, а в других – реализовываться совместно. В договорных соглашениях между организациями, участвующими в предоставлении или использовании услуг, следует четко оговорить сферы ответственности всех сторон в области защиты PII.

Средства управления, предусмотренные настоящей Спецификацией, могут применяться в качестве базовых средств организациями, обрабатывающими PII, и по своему замыслу применяться ко всем организациям, выступающим в роли диспетчеров PII. Организациям – обработчикам PII следует реализовывать средства управления в соответствии с указаниями диспетчеров PII. Диспетчеры PII должны обеспечить своим обработчикам PII возможность реализации всех необходимых средств управления, которые предусмотрены соглашением об обработке PII между диспетчером и обработчиком, в соответствии с целью обработки PII. Допускается, чтобы диспетчеры PII, использующие обработку PII облачными услугами, руководствовались стандартом ИСО/МЭК 27018 при определении подлежащих реализации средств управления.

Подробное разъяснение в отношении средств управления, предусмотренных настоящей Спецификацией, приведено в пп. 5–18 вместе с руководящими указаниями по их реализации. Реализацию можно упростить, если учесть требования к защите PII при проектировании информационной системы, услуг и операционной деятельности конкретной организации. Это является составной частью концепции, широко известной под названием "защита конфиденциальности на этапе проектирования". Более подробная информация о выборе средств управления и других способов противодействия рискам приведена в стандарте ИСО/МЭК 29134. Другие соответствующие ссылки по рассматриваемым здесь вопросам см. в разделе "Библиография".

4.5 Разработка руководящих указаний для конкретной организации

Настоящая Спецификация может служить отправной точкой для разработки руководящих указаний, предназначенных к применению в конкретной организации. Некоторые средства управления и руководящие указания из настоящей Спецификации применимы не ко всем организациям.

Более того, может возникнуть необходимость в дополнительных средствах управления и руководящих указаниях, не нашедших отражения в настоящей Спецификации. При разработке документов, которые устанавливают дополнительные средства управления или содержат дополнительные руководящие указания, может быть целесообразно дать перекрестные ссылки на положения настоящей Спецификации, если это применимо, тем самым облегчая задачу проверки соответствия для аудиторов и деловых партнеров.

4.6 Соображения, касающиеся жизненного цикла

Существует естественный жизненный цикл PII – от создания (генерации), сбора, хранения, использования и передачи до ее удаления (например, путем безопасного уничтожения). Ценность PII и риски, которым она подвергается, могут меняться на протяжении ее жизненного цикла, но защита PII остается важной в известной степени на всех этапах и во всех контекстах ее жизненного цикла.

И у информационных систем есть свой жизненный цикл, в пределах которого существуют следующие этапы: формирование замысла, определение технических условий, проектирование, разработка, испытания, внедрение, эксплуатация, обслуживание, вывод из эксплуатации и утилизация. На каждом из этих этапов также следует принимать во внимание требования защиты PII. При разработке новых и модификации существующих информационных систем у организаций появляется возможность скорректировать и усовершенствовать средства управления безопасностью и средства управления для защиты PII с учетом предшествующих инцидентов, а также текущих и прогнозируемых рисков для информационной безопасности и защиты конфиденциальности.

4.7 Структура настоящей Спецификации

Дальнейший текст настоящей Спецификации состоит из двух основных нормативных частей.

Первая часть Спецификации, которую составляют разделы 5–18, содержит дополнительные руководящие указания по реализации некоторых существующих средств управления, описанных в стандарте ИСО/МЭК 27002, и сопутствующую информацию. Заголовки и нумерация разделов для этой части соответствуют тем, которые даны в стандарте ИСО/МЭК 27002, и это обеспечивает возможность перекрестных ссылок на данный Международный стандарт.

Вторая часть содержит конкретное средство управления для защиты PII, описываемое в Приложении A. В ней используется тот же формат, что и в стандарте ИСО/МЭК 27002; определяется задача по защите PII (текст в рамке), а за ней – одно или несколько средств управления, которые могут быть приняты для ее решения. Описание средства управления имеет следующую структуру.

Средство управления

В тексте под данным заголовком приводится описание конкретного средства управления, предназначенного для решения соответствующей задачи по управлению.

Руководящие указания по реализации в целях защиты PII

В тексте под данным заголовком приводится более подробная информация, призванная помочь в реализации данного средства управления и решении соответствующей задачи по управлению. Руководящие указания, изложенные в настоящей Спецификации, могут быть не вполне пригодными или недостаточными в определенных ситуациях, а также могут не отвечать предъявляемым в организации конкретным требованиям к данному средству управления. В этом случае могут оказаться целесообразными другие или дополнительные средства управления либо иные формы противодействия рискам, такие как избежание или переадресация рисков.

Иная информация для защиты PII

В тексте под данным заголовком приводится другие сведения, учет которых может быть необходим, например юридические соображения и ссылки на другие стандарты.

5 Политика информационной безопасности

5.1 Руководящие указания по обеспечению информационной безопасности

5.1.1 Введение

См. задачу, определяемую в пункте 5.1 стандарта ИСО/МЭК 27002:2013.

5.1.2 Политика информационной безопасности

См. средство управления, определяемое в пункте 5.1.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иная информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Политика информационной безопасности должна включать надлежащие заявления о мерах безопасности для защиты PII. Подробную информацию о защите PII см. в пункте 18.1.4 ИСО/МЭК 27002:2013.

При разработке, реализации и пересмотре политики информационной безопасности организациям следует учитывать требования защиты конфиденциальности, изложенные в ИСО/МЭК 29100.

Организациям следует определить элементы защиты PII, которые не связаны с безопасностью, как отдельную политику обеспечения конфиденциальности. См. руководяще указание в пункте A.2.

5.1.3 Пересмотр политики информационной безопасности

См. средство управление, определяемое в пункте 5.1.2 стандарта ИСО/МЭК 27002, и соответствующие руководящие указания по его реализации.

6 Организация обеспечения информационной безопасности

6.1 Внутренняя организация

6.1.1 Введение

См. задачу, определяемую в пункте 6.1 стандарта ИСО/МЭК 27002.

6.1.2 Распределение ролей и ответственности в сфере информационной безопасности

См. средство управления, определяемое в пункте 6.1.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Необходимо четко определить, надлежащим образом задокументировать и довести до сведения персонала распределение ролей и ответственности для защиты PII. В частности:

a) следует назначить конкретное лицо из числа руководящего состава ответственным за защиту PII в организации (иногда это может быть руководитель службы обеспечения конфиденциальности информации, CPO);

b) следует назначить конкретное лицо или группу лиц ответственными за координацию деятельности с функциональными подразделениями информационной безопасности в данной организации (то есть создать функциональное подразделение защиты PI);

c) для всех отдельных лиц, занимающихся обработкой PII (включая пользователей и персонал службы технической поддержки), следует предусмотреть соответствующие требования к защите PII в квалификационных требованиях ко всем должностям.

Созданное функциональное подразделение защиты PII должно работать в тесном сотрудничестве с другими функциональными подразделениями, занимающимися обработкой PII, – в частности, с подразделением информационной безопасности, которое обеспечивает реализацию требований безопасности, диктуемых законодательством о защите PII, и с юридическим подразделением, которое содействует в толковании нормативно-правовых актов и условий договоров, а также в реагировании на утечки данных.

Данной организации следует изучить вопрос о необходимости создания многофункционального совета или комитета из числа руководящего состава функциональных подразделений, занимающихся обработкой PII, и в случае положительного решения создать такую группу. Учитывая многофункциональный характер защиты PII, эта группа может помочь в упреждающем поиске

возможностей для усовершенствования, выявлении новых рисков и сфер для проведения PIA, а также в планировании профилактических мероприятий, мер по обнаружению утечек и реагированию на них и т. д. Рекомендуется периодически проводить собрания такой группы под председательством лица, ответственного за защиту PII согласно пункту (a).

Диспетчеру PII следует потребовать от своих обработчиков PII назначить контактное лицо для обращения по вопросам обработки PII в рамках соответствующего договора на обработку.

Лица, ответственные за выполнение функций по защите PII, должны быть подотчетны CPO, чтобы обладать достаточными полномочиями для выполнения задач, входящих в сферу их ответственности.

6.1.3 Разграничение обязанностей

См. средство управления, определяемое в пункте 6.1.2 стандарта ИСО/МЭК 27002, и сопутствующие руководящие указания по его реализации. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Важно в максимально возможной степени разграничить обязанности и сферу ответственности в областях защиты PII и информационной безопасности, невзирая на существенную роль информационной безопасности в защите PII. Если это необходимо или полезно для защиты PII, следует наладить координацию и сотрудничество между лицами, ответственными за информационную безопасность и защиту PII.

Организациям следует внедрить принцип разграничения обязанностей при назначении прав доступа для целей обработки PII (особенно тех видов ее обработки, которые характеризуются высокой степенью риска).

В частности, следует разграничить обязанности, связанные с доступом к обрабатываемой PII и к файлам журналов ее обработки.

Доступ к информации о сборе PII для ответа на запросы, поступающие от субъектов PII, следует отделить от всех прочих форм доступа к PII; предоставлять доступ следует только тем лицам, которым поручена обязанность отвечать на такие запросы.

6.1.4 Взаимодействие с органами власти

См. средство управления, определяемое в пункте 6.1.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Там, где это применимо, организациям следует установить процедуры, определяющие, кто и в каких случаях должен обращаться в органы власти (включая органы по защите данных), например для того, чтобы сообщить об утечке конфиденциальной информации или отчитаться о деталях обработки.

6.1.5 Взаимодействие со специальными группами по интересам

См. средство управления, определяемое в пункте 6.1.4 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

6.1.6 Информационная безопасность в управлении проектами

См. средство управления, определяемое в пункте 6.1.5 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

При запуске любого нового проекта следует проводить как минимум пороговый анализ для определения потребности в PIA. Следует отметить, что под термином "проект" подразумеваются все случаи, когда та или иная организация внедряет новые или модифицирует имеющиеся технологии, продукты, услуги, программы, информационные системы, процессы или проекты в узком смысле.

Дальнейшие указания см. в стандарте ИСО/МЭК 29134 по вопросам проведения PIA.

6.2 Мобильные устройства и телеработа

6.2.1 Введение

См. задачу, определенную в пункте 6.2 стандарта ИСО/МЭК 27002:2013.

6.2.2 Политика в отношении мобильных устройств

См. средство управления, определяемое в пункте 6.2.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Организациям следует строго ограничить доступ к PII с переносных и мобильных устройств, таких как ноутбуки, мобильные телефоны, устройства с универсальной последовательной шиной (USB) и персональные цифровые помощники (PDA), которые в общем случае подвержены бóльшему риску, чем стационарные устройства (например, настольные компьютеры, установленные в принадлежащих организации помещениях), в зависимости от результата оценки рисков.

Организациям следует также строго ограничить удаленный доступ к PII, а в случаях, когда такой доступ неизбежен, – обеспечить шифрование и защиту целостности передаваемых данных, а также аутентификацию сообщений.

6.2.3 Телеработа

См. средство управления, определяемое в пункте 6.2.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

7 Безопасность кадровых ресурсов

7.1 Перед приемом на работу

7.1.1 Введение

См. задачу, изложенную в пункте 7.1 стандарта ИСО/МЭК 27002:2013.

7.1.2 Отбор штатного состава

См. средство управления, определяемое в пункте 7.1.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

7.1.3 Сроки и условия работы по найму

См. средство управления, определяемое в пункте 7.1.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

7.2 В период работы по найму

7.2.1 Введение

См. задачу, изложенную в пункте 7.2 стандарта ИСО/МЭК 27002:2013.

7.2.2 Сфера ответственности руководства

См. средство управления, определяемое в пункте 7.2.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

7.2.3 Информирование, обучение и подготовка в области информационной безопасности

См. средство управления, определяемое в пункте 7.2.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Следует довести до сведения соответствующего персонала возможные последствия нарушения правил и процедур защиты конфиденциальности или безопасности для диспетчера PII (например, правовые

последствия, потерю клиентов, ущерб для бренда или репутации), членов персонала (например, дисциплинарные меры) и субъекта PII (например, физический, материальный и моральный ущерб), особенно тех правил и процедур, которые относятся к обработке PII.

Организациям следует обеспечить надлежащие информирование, обучение и подготовку в области защиты и обработки PII подобно тому, как это делается в области информационной безопасности.

7.2.4 Дисциплинарный процесс

См. средство управления, определяемое в пункте 7.2.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Организациям следует установить официальную дисциплинарную политику в отношении утечки конфиденциальной информации. Эту политику следует довести до сведения всех лиц, которых она затрагивает, и проводить в жизнь во всех случаях, когда происходит такая утечка.

7.3 Увольнение и перемещение на места работы

7.3.1 Введение

См. задачу, изложенную в пункте 7.3 стандарта ИСО/МЭК 27002:2013.

7.3.2 Увольнение или перемещение на места работы

См. средство управления, определяемое в пункте 7.3.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

8 Управление активами

8.1 Ответственность за активы

8.1.1. Введение

См. задачу, изложенную в пункте 8.1 стандарта ИСО/МЭК 27002:2013.

8.1.2 Инвентаризация активов

См. средство управления, определяемое в пункте 8.1.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Организациям следует составлять, вести и обновлять инвентарный перечень активов, используя, например, информацию из отчета по результатам оценки воздействия на конфиденциальность (PIA) в соответствии со стандартом ИСО/МЭК 29134 (если такой отчет имеется). В этот перечень должны входить информационные активы PII и все системы, в которых обрабатывается PII.

При составлении и ведении такого инвентарного перечня организациям следует использовать по результатам оценки следующие сведения об информационных системах, в которых обрабатывается PII (нижеследующий список приведен для примера – в окончательной редакции он может быть расширен или сокращен):

a) полное и сокращенное наименование каждой выявленной системы;

b) типы PII, которая обрабатывается в этих системах;

c) классификация (см. пункт 8.2.2) всех типов PII, как отдельных элементов информации, так и их совокупности в этих информационных системах;

d) потенциальный уровень воздействия утечек PII на субъекта PII и организацию;

e) цели сбора PII;

f) планируется ли отдать обработку PII на внешний подряд;

g) передается ли PII другим диспетчерам PII, и если да, то каким (или какой группе получателей);

h) срок хранения PII;

i) географический район, в котором собиралась или обрабатывалась PII; и

j) имела ли место трансграничная передача данных.

Организации должны регулярно предоставлять обновленные данные по инвентарному перечню PII лицу, ответственному за защиту PII, для содействия принятию надлежащих средств управления безопасностью в отношении всех новых и модифицированных информационных систем, в которых обрабатывается PII.

8.1.3 Владение активами

См. средство управления, определяемое в пункте 8.1.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

8.1.4 Допустимые способы использования активов

См. средство управления, определяемое в пункте 8.1.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Организациям следует обеспечить защиту активов, поддерживающих PII, от несанкционированного доступа, модификации, удаления, потери и/или уничтожения, ненадлежащей или незаконной обработки и других угроз.

8.1.5 Возврат активов

См. средство управления, определяемое в пункте 8.1.4 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

8.2 Классификация информации

8.2.1 Введение

См. задачу, изложенную в пункте 8.2 стандарта ИСО/МЭК 27002:2013.

8.2.2 Классификация информации

См. средство управления, определяемое в пункте 8.2.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Организациям следует классифицировать всю информацию, содержащую PII, используя существующую классификационную категорию (называемую в ИСЭ/МЭК 27002 информационной группой). Новые классификационные категории могут включать, в том числе, общие, например конфиденциальная и не конфиденциальная PII. Схема классификации может включать также более конкретные категории, такие как личная медицинская информация (PHI), личная финансовая информация (PFI). Создавая новые классификационные категории, организация должна определять также их уровни защиты. Перечень используемых фактических категорий должен зависеть также, например, от требований, установленных применимыми нормативно-правовыми актами о защите данных, другими правовыми (например, договорными) обязательствами, характером и степенью конфиденциальности информации, а также риском возможного ущерба в случае утечки.

Некоторые типы PII могут классифицироваться как не конфиденциальные в одной стране и как конфиденциальные в другой в зависимости от требований применимого законодательства о защите данных.

Если отдельный элемент PII связывается с одним или несколькими дополнительными атрибутами, это может привести к необходимости пересмотра и изменения его классификации. Для таких случаев следует разработать соответствующие руководящие указания и процедуры.

8.2.3 Маркировка информации

См. средство управления, определяемое в пункте 8.2.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Если организация не относит PII к какой-либо классификационно категории, она должна обеспечить, чтобы лица, находящиеся под ее контролем, были осведомлены об определении PII и способах выявления PII.

8.2.4 Обращение с активами

См. средство управления, определяемое в пункте 8.2.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Если организация разрешает лицам, находящимся под ее контролем, опускать международную маркировку классификационной категории, относящейся к PII, она должна обязать лиц, находящихся под ее контролем, обрабатывать всю информацию, содержащую PII, как информацию назначенной классификационной категории.

8.3 Обращение с носителями данных

8.3.1 Введение

См. задачу, изложенную в пункте 8.3 стандарта ИСО/МЭК 27002:2013.

8.3.2 Обращение со съемными носителями данных

См. средство управления, определяемое в пункте 8.3.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

В некоторых юрисдикциях может требоваться обязательное шифрование данных на съемных носителях с PII. Даже в случаях отсутствия соответствующих законодательных требований рекомендуется шифровать данные для снижения риска утечки PII.

Если важны конфиденциальность или целостность данных, следует защищать PII на съемных носителях, используя методы шифрования. Предварительно следует провести оценку рисков, чтобы определить требуемый уровень защиты, от которого в свою очередь зависит выбор типа, эффективности и качества используемого алгоритма шифрования.

Дополнительные руководящие указания, касающиеся средств управления с использованием шифрования, приведены в пункте 10.1.

8.3.3 Утилизация носителей данных

См. средство управления, определяемое в пункте 8.3.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Процедуры безопасной утилизации носителей, содержащих PII, должны соответствовать чувствительности этой информации, а также уровню прогнозируемых последствий ее ненадлежащей обработки. В некоторых юрисдикциях могут устанавливаться обязательные требования к порядку

утилизации носителей, содержащих PII, или конкретные типы PII (например, медицинские данные, финансовые данные и т. д.).

8.3.4 Передача физических носителей данных

См. средство управления, определяемое в пункте 8.3.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

В случаях, когда информация передается на физических носителях, следует принять меры для регистрации входящих и исходящих физических носителей, содержащих PII, с указанием типа носителя, идентификационных номеров (например, серийных или инвентарных), авторизованных отправителя и получателей, даты и времени, количества физических носителей, типов содержащейся на них PII и физического состояния носителей, а также для обнаружения потерь в физических носителях. Кроме того, следует документально фиксировать цель и дальность передачи, лицо, ответственное за ее авторизацию, и правовые/договорные основания для ее передачи. Наконец, следует дополнительно рассмотреть возможность прямой ссылки на принцип минимизации объема данных.

9 Управление доступом

9.1 Бизнес-требования к управлению доступом

9.1.1 Введение

См. задачу, изложенную в пункте 9.1 стандарта ИСО/МЭК 27002:2013.

9.1.2 Политика управления доступом

См. средство управления, определяемое в пункте 9.1.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

9.1.3 Доступ к сетям и сетевым услугам

См. средство управления, определяемое в пункте 9.1.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

9.2 Управление доступом пользователей

9.2.1 Введение

См. задачу, изложенную в пункте 9.2 стандарта ИСО/МЭК 27002:2013.

9.2.2 Регистрация и снятие с регистрации пользователей

См. средство управления, определяемое в пункте 9.2.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Процедуры регистрации и снятия с регистрации пользователей, а также управления жизненным циклом информационной системы пользователя должны предусматривать меры реагирования на нарушение нормальной работы системы управления доступом пользователей, включая порчу или раскрытие паролей или других регистрационных данных (например, из-за непреднамеренного раскрытия).

9.2.3 Обеспечение доступа пользователя

См. средство управления, определяемое в пункте 9.2.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Организации должны предоставлять пользователям надлежащие права на доступ к информационным системам по обработке PII в соответствии с принципом минимизации объема данных, изложенным в стандарте ИСО/МЭК 29100.

Организациям следует ограничивать доступ к информационным системам по обработке PII, предоставляя его минимальному числу лиц, которое необходимо для выполнения определенных целей обработки согласно принципу минимизации объема данных, изложенному в стандарте ИСО/МЭК 29100.

Организациям следует внедрить эффективные методы аутентификации для обработки PII или конкретных типов PII (например, медицинских данных).

9.2.4 Управление правами привилегированного доступа

См. средство управления, определяемое в пункте 9.2.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Крупномасштабная обработка PII (например, пакетные запросы, изменение, экспорт и удаление пакетов) повышает риск крупномасштабной утечки. Организациям следует соблюдать особые меры предосторожности при назначении прав доступа для выполнения таких привилегированных операций. Чтобы избежать злоупотреблений в отношении PII, права привилегированного доступа для обработки PII (особенно обработки с высокими рисками) следует назначать с соблюдением строгих ограничений. Кроме того, назначать эти права следует так, чтобы уменьшить риск сговора между двумя или более лицами. Назначение и использование этих прав должно регистрироваться в соответствующих файлах журнала. Все разрешения на доступ следует предоставлять на определенный срок, а впоследствии регулярно пересматривать и по мере необходимости возобновлять, отзывать или прекращать действие таких разрешений.

9.2.5 Управление секретными аутентификационными данными пользователей

См. средство управления, определяемое в пункте 9.2.4 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

9.2.6 Пересмотр прав доступа пользователей

См. средство управления, определяемое в пункте 9.2.5 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

9.2.7 Отзыв или корректировка прав доступа

См. средство управления, определяемое в пункте 9.2.6 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

9.3 Сфера ответственности пользователей

9.3.1 Введение

См. задачу, изложенную в пункте 9.3 стандарта ИСО/МЭК 27002:2013.

9.3.2 Использование секретных аутентификационных данных

См. средство управления, определяемое в пункте 9.3.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

9.4 Управление доступом к системам и приложениям

9.4.1 Введение

См. задачу, изложенную в пункте 9.4 стандарта ИСО/МЭК 27002:2013.

9.4.2 Ограничение доступа к информации

См. средство управления, определяемое в пункте 9.4.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Прежде чем разрешать отдельным лицам, например операторам и администраторам, пользоваться языками запросов, которые допускают объемное извлечение PII из баз данных, организациям следует изучить вопрос о действительной необходимости использования таких языков при обработке PII.

В случае если использование языков запроса отвечает требованиям защиты PII, организациям следует принять технические меры для ограниченного использования таких языков тем минимумом, который необходим для указанных целей.

Например, возможность доступа с использованием языков запроса может быть ограничена установленным перечнем из нескольких полей с чувствительной информацией.

Для случаев, когда отдельным лицам требуется доступ к тем областям, которые для них обычно недоступны (например, к операционной области), следует внедрить надежные разрешительные механизмы. Организациям следует вести регистрацию всех полученных таким образом разрешений на доступ.

9.4.3 Процедуры безопасного входа в систему

См. средство управления, определяемое в пункте 9.4.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

В случаях, когда субъекты PII могут запрашивать учетные записи у диспетчера PII, диспетчеру следует реализовывать процедуры безопасного входа в систему с использованием этих учетных записей, основываясь на результатах оценки рисков.

9.4.4 Система управления паролями

См. средство управления, определяемое в пункте 9.4.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

9.4.5 Использование привилегированных служебных программ

См. средство управления, определяемое в пункте 9.4.4 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

9.4.6 Управление доступом к исходному коду программ

См. средство управления, определяемое в пункте 9.4.5 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

10 Шифрование

10.1 Средства управления, связанные с шифрованием

10.1.1 Введение

См. задачу, изложенную в пункте 10.1 стандарта ИСО/МЭК 27002:2013.

10.1.2 Политика в области применения средств управления, связанных с шифрованием

См. средство управления, определяемое в пункте 10.1.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

10.1.3 Управление ключами

См. средство управления, определяемое в пункте 10.1.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

11 Физическая безопасность и безопасность окружающей среды

11.1 Защищенные зоны

11.1.1 Введение

См. задачу, изложенную в пункте 11.1 стандарта ИСО/МЭК 27002:2013.

11.1.2 Периметр физической безопасности

См. средство управления, определяемое в пункте 11.1.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

11.1.3 Средства управления физическим доступом

См. средство управления, определяемое в пункте 11.1.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

11.1.4 Обеспечение безопасности офисов, помещений и оборудования

См. средство управления, определяемое в пункте 11.1.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

11.1.5 Защита от внешних угроз и угроз для окружающей среды

См. средство управления, определяемое в пункте 11.1.4 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

11.1.6 Работа в защищенных зонах

См. средство управления, определяемое в пункте 11.1.5 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

11.1.7 Зоны доставки и загрузки

См. средство управления, определяемое в пункте 11.1.6 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

11.2 Оборудование

11.2.1 Введение

См. задачу, изложенную в пункте 11.2 стандарта ИСО/МЭК 27002:2013.

11.2.2 Размещение и защита оборудования

См. средство управления, определяемое в пункте 11.2.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

11.2.3 Вспомогательное оборудование

См. средство управления, определяемое в пункте 11.2.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

11.2.4 Безопасность кабельных систем

См. средство управления, определяемое в пункте 11.2.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

11.2.5 Техническое обслуживание оборудования

См. средство управления, определяемое в пункте 11.2.4 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

11.2.6 Перемещение активов

См. средство управления, определяемое в пункте 11.2.5 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

11.2.7 Безопасность оборудования и активов за пределами территории организации

См. средство управления, определяемое в пункте 11.2.6 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

11.2.8 Безопасная утилизация или повторное использование оборудования

См. средство управления, определяемое в пункте 11.2.7 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

В целях безопасной утилизации или повторного использования оборудования следует либо физически уничтожать оборудование, в составе которого имеются носители данных, могущие содержать PII, либо уничтожать, удалять или затирать PII согласно четко определенным и документированным процедурам и с применением утвержденных методов вместо использования функции стандартного удаления или форматирования, чтобы исключить возможность последующего восстановления исходной PII. Для оборудования, в составе которого имеются носители данных, могущие содержать PII в зашифрованном виде, достаточной мерой может быть контролируемое уничтожение ключей шифрования и/или носителей таких ключей (например, смарт-карт).

11.2.9 Оборудование пользователя, оставленное без присмотра

См. средство управления, определяемое в пункте 11.2.8 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

11.2.10 Процедуры уборки рабочих мет и очистки экранов

См. средство управления, определяемое в пункте 11.2.9 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

12 Эксплуатационная безопасность

12.1 Эксплуатационные процедуры и сферы ответственности

12.1.1 Введение

См. задачу, изложенную в пункте 12.1 стандарта ИСО/МЭК 27002:2013.

12.1.2 Документирование эксплуатационных процедур

См. средство управления, определяемое в пункте 12.1.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

12.1.3 Управление изменениями

См. средство управления, определяемое в пункте 12.1.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

12.1.4 Управление пропускной способностью

См. средство управления, определяемое в пункте 12.1.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

12.1.5 Разграничение сред проектирования, тестирования и эксплуатации

См. средство управления, определяемое в пункте 12.1.4 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Среды проектирования, тестирования и эксплуатации следует разграничить логически, а там, где это возможно, также и физически. При этом следует реализовать надлежащие средства управления доступом, чтобы доступ предоставлялся только лицам, которые обладают надлежащими полномочиями. Если для функционирования сетей или устройств как тестовых, так и для целей проектирования требуется доступ к эксплуатационной сети, следует реализовать высокоэффективные средства управления доступом.

Организации следует оценить риск, связанный с использованием съемных носителей и устройств с возможностями беспроводного доступа, вне зависимости от среды, в которой они будут использоваться.

Не следует использовать PII для целей проектирования и тестирования без предварительного ее обезличивания в случаях, когда это запрещено законом или когда субъект PII не дал на это явного согласия.

12.2 Защита от вредоносного программного обеспечения

12.2.1 Введение

См. задачу, изложенную в пункте 12.2 стандарта ИСО/МЭК 27002:2013.

12.2.2 Средства управления для защиты от вредоносного программного обеспечения

См. средство управления, определяемое в пункте 12.2.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

12.3 Резервное копирование

12.3.1 Введение

См. задачу, изложенную в пункте 12.3 стандарта ИСО/МЭК 27002:2013.

12.3.2 Резервное копирование информации

См. средство управления, определяемое в пункте 12.3.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

В информационных системах, используемых для обработки PII, следует предусматривать дополнительные или альтернативные механизмы, такие как механизмы удаленного резервного копирования для защиты от потерь PII, обеспечения непрерывного выполнения операций по обработке PII и обеспечения возможности их возобновления после событий, нарушающих работу, только в том случае, если это строго необходимо.

ПРИМЕЧАНИЕ. – Между операциями резервного копирования и восстановления проходит определенное время. Версия PII, содержащаяся в резервной копии, может устареть на момент восстановления. Любые операции с устаревшей PII могут привести к неверным результатам и создать риск нарушения конфиденциальности.

12.4 Ведение журнала и мониторинг

12.4.1 Введение

См. задачу, изложенную в пункте 12.4 стандарта ИСО/МЭК 27002:2103.

12.4.2 Ведение журнала событий

См. средство управления, определяемое в пункте 12.4.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

По возможности следует записывать в журнал событий сведения о том, какие операции (например, чтение, печать, добавление, изменение, удаление), с какой именно PII, когда и кем выполнялись, особенно в отношении некоторых типов PII (например, медицинских данных). Если услугу оказывают совместно несколько поставщиков услуг, они могут разграничить между собой роли в осуществлении этих руководящих указаний или выполнять некоторые роли сообща.

Следует организовать регулярный просмотр журнала событий с установленной и документально зафиксированной периодичностью, с тем чтобы выявлять отклонения от нормы и вносить предложения по исправлению ситуации.

Диспетчеру PII следует определить процедуры, касающиеся того, может ли информация из журналов событий стать доступной или использоваться администратором для целей мониторинга безопасности и эксплуатационной диагностики, и если да, то когда и в каком порядке.

12.4.3 Защита информации в файлах журналов

См. средство управления, определяемое в пункте 12.4.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Информация, которая записывается в журналы для целей мониторинга и эксплуатационной диагностики, может в числе прочего содержать PII. Чтобы эта информация из журналов использовалась только для установленных целей, следует принять надлежащие меры, такие как управление доступом (см. пункт 9.2.3). Кроме того, следует принять меры для обеспечения целостности файлов журналов.

12.4.4 Журналы работы администраторов и операторов

См. средство управления, определяемое в пункте 12.4.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Организациям следует вести мониторинг привилегированного доступа к PII (например, со стороны системных администраторов и операторов) и последующей ее обработки этими лицами. Такой мониторинг должен составлять часть общего мониторинга информационных систем, в которых обрабатывается PII.

Организациям следует определить, какие действия должны считаться ненадлежащими, и внедрить автоматизированные процедуры для направления отчетов о таких действиях компетентным сотрудникам организации.

12.4.5 Синхронизация времени

См. средство управления, определяемое в пункте 12.4.4 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

12.5 Управление системным программным обеспечением

12.5.1 Введение

См. задачу, изложенную в пункте 12.5 стандарта ИСО/МЭК 27002:2013.

12.5.2 Установка программного обеспечения в операционных системах

См. средство управления, определяемое в пункте 12.5.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

12.6 Управление техническими уязвимостями

12.6.1 Введение

См. задачу, изложенную в пункте 12.6 стандарта ИСО/МЭК 27002:2013.

12.6.2 Управление техническими уязвимостями

См. средство управления, определяемое в пункте 12.6.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

12.6.3 Ограничения на установку программного обеспечения

См. средство управления, определяемое в пункте 12.6.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

12.7 Соображения, касающиеся аудита информационных систем

12.7.1 Введение

См. задачу, изложенную в пункте 12.7 стандарта ИСО/МЭК 27002:2013.

12.7.2 Средства управления для аудита информационных систем

См. средство управления, определяемое в пункте 12.7.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

13 Безопасность связи

13.1 Управление безопасностью сетей

13.1.1 Введение

См. задачу, изложенную в пункте 13.1 стандарта ИСО/МЭК 27002:2013.

13.1." Средства управления сетями

См. средство управления, определяемое в пункте 13.1.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

13.1.3 Безопасность сетевых услуг

См. средство управления, определяемое в пункте 13.1.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

13.1.4 Разделение сетей

См. средство управления, определяемое в пункте 13.1.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

13.2 Передача информации

13.2.1 Введение

См. задачу, изложенную в пункте 13.2 стандарта ИСО/МЭК 27002:2013.

13.2.2 Правила и процедуры передачи информации

См. средство управления, определяемое в пункте 13.2.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Следует принять надлежащие меры для уменьшения риска утечки PII во время передачи информации. Обычно эта задача решается внедрением методов шифрования. Другие возможные предварительные меры – удаление идентифицирующих элементов, маскирование или запутывание.

13.2.3 Соглашения о передаче информации

См. средство управления, определяемое в пункте 13.2.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

13.2.4 Электронная передача сообщений

См. средство управления, определяемое в пункте 13.2.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

13.2.5 Соглашение о конфиденциальности или неразглашении информации

См. средство управления, определяемое в пункте 13.2.4 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Организациям следует определить условия, при которых допускается внешняя обработка PII. Эти условия должны быть оговорены в соответствующем соглашении (например, в договоре, соглашении о конфиденциальности или неразглашении информации).

14 Приобретение, развитие и техническое обслуживание информационных систем

14.1 Требования к безопасности информационных систем

14.1.1 Введение

См. задачу, изложенную в пункте 14.1 стандарта ИСО/МЭК 27002:2013.

14.1.2 Анализ и определение требований информационной безопасности

См. средство управления, определяемое в пункте 14.1.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

В процессе развития или существенной модификации информационных систем, в которых обрабатывается PII, следует проводить оценку воздействия на конфиденциальность (PIA). Руководящие указания по проведению такой оценки излагаются в стандарте ИСО/МЭК 29134. Исходя из результатов PIA следует определить средства управления для противодействия выявленным в ходе процесса PIA рискам.

14.1.2 Обеспечение безопасности прикладных услуг в сетях общего пользования

См. средство управления, определяемое в пункте 14.1.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

14.1.3 Защита транзакций прикладных услуг

См. средство управления, определяемое в пункте 14.1.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

14.2 Обеспечение безопасности в процессах развития и технической поддержки

14.2.1 Введение

См. задачу, изложенную в пункте 14.2 стандарта ИСО/МЭК 27002:2013.

14.2.2 Политика безопасного развития

См. средство управления, определяемое в пункте 14.2.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

14.2.3 Процедуры управления изменениями в системах

См. средство управления, определяемое в пункте 14.2.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

14.2.4 Технический пересмотр приложений после внесения изменений в операционную платформу

См. средство управления, определяемое в пункте 14.2.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

14.2.5 Ограничения на изменения в программных пакетах

См. средство управления, определяемое в пункте 14.2.4 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

14.2.6 Принципы проектирования безопасных систем

См. средство управления, определяемое в пункте 14.2.5 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

14.2.7 Среда безопасной разработки

См. средство управления, определяемое в пункте 14.2.6 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

14.2.8 Разработка силами сторонних организаций

См. средство управления, определяемое в пункте 14.2.7 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

14.2.9 Испытания систем на безопасность

См. средство управления, определяемое в пункте 14.2.8 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

14.2.10 Приемо-сдаточные испытания систем

См. средство управления, определяемое в пункте 14.2.9 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

В программу приемо-сдаточных испытаний системы следует включить проверку соблюдения требований защиты конфиденциальности.

14.3 Тестовые данные

14.3.1 Введение

См. задачу, изложенную в пункте 14.3 стандарта ИСО/МЭК 27002:2013.

14.3.2 Защита тестовых данных

См. средство управления, определяемое в пункте 14.3.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

В обычных условиях не следует использовать для разработки и тестирования оперативные данные, содержащие PII. Использование реальной PII в этих режимах повышает риск того, что информация будет раскрыта. Для указанных целей организациям следует использовать синтезированные данные или же принять меры к скрытию (маскированию, запутыванию, удалению идентифицирующих элементов и т. д.) реальной используемой PII.

15 Взаимоотношения с поставщиками

15.1 Информационная безопасность во взаимоотношениях с поставщиками

15.1.1 Введение

См. задачу, изложенную в пункте 15.1 стандарта ИСО/МЭК 27002:2013.

15.1.2 Политика информационной безопасности во взаимоотношениях с поставщиками

См. средство управления, определяемое в пункте 15.1.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

В случае если организации требуются услуги обработчика PII, то оценивать кандидатов следует на основании опыта, надежности и способности выполнить требования к защите PII, установленные нормативно-правовыми актами, договорами или другими юридическими соглашениями.

Организации, действующей в качестве диспетчера PII, следует заключить письменный договор со всеми поставщиками, которым она поручает роль обработчиков PII. В договоре следует четко распределить роли и обязанности между диспетчером и обработчиком PII, а также предусмотреть соответствующие положения о защите PII, чтобы установить ответственность обработчика PII за выполняемую обработку.

Положения договора между диспетчером и обработчиком PII должны предусматривать по крайней мере следующее:

- надлежащее определение масштаба, характера и целей обработки по договору;
- вспомогательные обязанности обработчика PII предоставлять субъектам PII возможности доступа к затрагивающей их PII и ее пересмотра, а также обрабатывать жалобы, поступающие от субъектов PII (см. пункт A.10);
- другие организационные меры, которые должны быть приняты для выполнения регуляторных требований;
- разрешение диспетчеру PII осуществлять аудит в помещении организации – обработчика PII;
- обязательства сообщать об утечках данных, несанкционированной обработке и других случаях невыполнения сроков и условий договора с указанием контактных данных обеих сторон;
- способ передачи указаний от диспетчера PII обработчику PII;
- меры, применяемые при прекращении действия договора, в особенности меры по безопасному удалению PII в помещениях обработчика и/или по возврату PII и физических носителей.

Диспетчеру PII следует обеспечить, чтобы действующие по договору с ним обработчики PII не передавали обработку PII на дальнейший субподряд (то есть использование суб-обработчиков) без предварительного согласования с диспетчером. Диспетчер PII должен соблюдать требования всех применимых в этом отношении нормативно-правовых актов.

Диспетчеру PII следует обеспечить, чтобы действующие по договору с ним обработчики PII не обрабатывали PII для иных целей, кроме тех, которые установлены договором или другим юридическим соглашением.

Диспетчеру PII следует обеспечить, чтобы действующие по договору с ним обработчики PII безопасно изъяли PII в соответствии с политикой диспетчера или другими директивными документами (например, требованиями тех или иных конкретных органов).

15.1.3 Положения о безопасности в соглашениях с поставщиками

См. средство управления, определяемое в пункте 15.1.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

15.1.4 Логистическая цепочка средств информационно-коммуникационных технологий

См. средство управления, определяемое в пункте 15.1.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

15.2 Управление оказанием услуг, предоставляемых поставщиками

15.2.1 Введение

См. задачу, изложенную в пункте 15.2 стандарта ИСО/МЭК 27002:2013.

15.2.2 Мониторинг и пересмотр услуг, предоставляемых поставщиками

См. средство управления, определяемое в пункте 15.2.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

15.2.3 Управление изменениями в услугах, предоставляемых поставщиками

См. средство управления, определяемое в пункте 15.2.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

16 Управление инцидентами в области информационной безопасности

16.1 Управление инцидентами в области информационной безопасности и повышением информационной безопасности

16.1.1 Введение

См. задачу, изложенную в пункте 16.1 стандарта ИСО/МЭК 27002:2013.

16.1.2 Сфера ответственности и процедуры

См. средство управления, определяемое в пункте 16.1.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Организации должны быть способны и готовы к организованному и эффективному реагированию на инциденты, связанные с нарушением конфиденциальности. В связи с этим организациям следует разработать и ввести в действие план реагирования на такие инциденты.

План реагирования организации на инциденты, связанные с нарушением конфиденциальности, должен включать:

a) определение инцидента, связанного с нарушением конфиденциальности, а также рамки реагирования на инцидент, связанный с нарушением конфиденциальности

b) создание многофункциональной группы реагирования на инциденты, связанные с нарушением конфиденциальности, в задачи которой входит разработка, внедрение, тестирование, выполнение и пересмотр соответствующего плана реагирования (утверждение плана следует возложить на высшее руководство организации);

c) четкое распределение ролей, сфер ответственности и полномочий всех членов многофункциональной группы реагирования на инциденты, связанные с нарушением конфиденциальности;

d) процедуры прояснения правовых оснований для сотрудничества с внешними организациями (национальными и международными) в случае трансграничных инцидентов;

e) процедуры, которые обеспечивают, чтобы все лица, на которых распространяется внутренняя политика защиты конфиденциальности (то есть сотрудники, подрядчики), незамедлительно сообщали обо всех инцидентах, связанных с нарушением конфиденциальности, должностным лицам, ответственным за информационную безопасность, и лицу, ответственному за защиту PII (иногда называемому CPO) в соответствии с директивными правилами управления инцидентами в организации;

f) перечень задач по оценке последствий инцидентов в целях определения характера и масштаба потенциального или реального ущерба затронутым в результате инцидента лицам (например, конфуз, неудобство или несправедливость) или конкретной организации;

g) процесс определения мер, которые необходимо предпринять для снижения указанного выше ущерба и уменьшения вероятности его повторения в будущем; и

h) процедуры для определения необходимости, сроков и форм уведомления затронутых лиц и других назначенных структур (например, регуляторных органов), а также собственно процедуры такого уведомления в случаях, когда оно необходимо.

Организации по своему выбору могут объединить свои планы реагирования на инциденты, связанные с нарушением конфиденциальности, с планами реагирования на инциденты в области информационной безопасности или выполнять их по отдельности. Инцидент в области информационной безопасности должен приводить к расследованию данного события со стороны диспетчера PII в рамках установленного процесса управления такими инцидентами, с тем чтобы выяснить, произошла ли утечка данных, содержащих PII.

В отличие от указанного выше инцидента событие в области информационной безопасности не обязательно должно приводить к такому расследованию. К событиям в области информационной безопасности относят, среди прочего, запросы ping и другие широковещательные атаки на брандмауэры или пограничные серверы, сканирование портов, неудачные попытки входа в систему, атаки типа "отказ в обслуживании" и анализ пакетов. Событие в области информационной безопасности не обязательно приводит к вероятному или фактическому раскрытию PII либо оборудования (объектов), на которых обрабатывается PII.

16.1.3 Уведомление о событиях в области информационной безопасности

См. средство управления, определяемое в пункте 16.1.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

В случае раскрытия PII необходимо немедленно принять соответствующие меры, иначе невозможно будет защитить права и интересы субъекта PII.

В некоторых юрисдикциях посредством нормативно-правовых актов могут устанавливаться конкретные требования к отчетности и/или уведомлению об инцидентах в области информационной безопасности, связанных с PII (несанкционированная обработка, утечка данных и т. д.). Когда происходит инцидент в области информационной безопасности, связанный с PII, следует в кратчайшие сроки подробно уведомить затронутых инцидентом лиц и компетентные органы об этом инциденте, в том числе о предлагаемых организацией мерах реагирования (раскрытие которых может быть предметом определенных ограничений). В число компетентных органов могут входить органы по защите данных и правоохранительные органы.

В случае утечки информации, связанной с нарушением конфиденциальности, организации должны предоставить затронутым субъектам PII надлежащие и эффективные средства защиты, например возможность исправить или удалить неверную информацию.

16.1.4 Уведомление о слабых местах в системе обеспечения безопасности

См. средство управления, определяемое в пункте 16.1.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

16.1.5 Оценка событий в области информационной безопасности и принятие по ним решений

См. средство управления, определяемое в пункте 16.1.4 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

16.1.6 Реагирование на инциденты в области информационной безопасности

См. средство управления, определяемое в пункте 16.1.5 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

16.1.7 Извлечение уроков из инцидентов в области информационной безопасности

См. средство управления, определяемое в пункте 16.1.6 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

16.1.8 Сбор доказательств

См. средство управления, определяемое в пункте 16.1.7 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

17 Аспекты информационной безопасности как фактор управления для обеспечения непрерывности деятельности

17.1 Непрерывность обеспечения информационной безопасности

17.1.1 Введение

См. задачу, изложенную в пункте 17.1 стандарта ИСО/МЭК 27002:2013.

17.1.2 Планирование непрерывного обеспечения информационной безопасности

См. средство управления, определяемое в пункте 17.1.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

17.1.3 Реализация непрерывного обеспечения информационной безопасности

См. средство управления, определяемое в пункте 17.1.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

17.1.4 Проверка, пересмотр и оценка непрерывности обеспечения информационной безопасности

См. средство управления, определяемое в пункте 17.1.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

17.2 Избыточность

17.2.1 Введение

См. задачу, изложенную в пункте 17.2 стандарта ИСО/МЭК 27002:2013.

17.2.2 Доступность средств обработки информации

См. средство управления, определяемое в пункте 17.2.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

18 Соответствие требованиям

18.1 Соответствие законодательным и договорным требованиям

18.1.1 Введение

См. задачу, изложенную в пункте 18.1 стандарта ИСО/МЭК 27002:2013.

18.1.2 Выявление применимых законодательных и договорных требований

См. средство управления, определяемое в пункте 18.1.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

Организациям следует выяснить, какие нормативно-правовые акты, связанные с защитой PII, на них распространяются. Выяснив это, организации должны принять соответствующие меры для выполнения данных требований. Ниже приведены примеры таких требований.

a) В случае если требуется дополнительная защита некоторых категорий PII (например, государственного идентификационного номера, номера паспорта или кредитной карты), следует использовать методы криптографии, такие как шифрование. Требуемые тип, эффективность и качество криптографического алгоритма следует определять по результатам анализа рисков. Выбирать криптографический алгоритм следует только из перечней утвержденных алгоритмов.

См. средство управления, определяемое в пункте 10.1.2.

b) В некоторых юрисдикциях может устанавливаться минимальная периодичность резервного копирования информации, содержащей PII, а также минимальная периодичность пересмотра процедур резервного копирования и восстановления.

См. средство управления, определяемое в пункте 12.3.2.

Организациям также следует разработать процедуры PIA и по результатам таких оценок ввести в действие планы защиты конфиденциальности, помогающие обеспечить соответствие программ и услуг, связанных с обработкой PII, требованиям защиты конфиденциальности. Дальнейшие руководящие указания см. в стандарте ИСО/МЭК 29134.

Организациям следует ввести в действие программу аудита, помогающую удостовериться, что обработка PII соответствует применимым требованиям защиты конфиденциальности. Данная программа должна устанавливать периодичность проведения такого аудита.

Аудит может производиться как самой организацией (например, силами внутреннего аудиторского подразделения), так и квалифицированной независимой сторонней организацией.

Сопутствующая информация для защиты PII

Во многих юрисдикциях ответственность за обеспечение соответствия требованиям в конечном счете возлагается на диспетчера PII. Тем не менее всем сторонам, участвующим в обработке PII, следует принять упреждающий подход к выявлению применимых требований защиты конфиденциальности, вытекающих из законов или других факторов.

Механизм, обеспечивающий для обработчика PII возможность поддержания и управления соответствием, устанавливается договором между диспетчером и обработчиком PII. В договоре следует предусмотреть независимый аудит соответствия в приемлемом для обработчика PII формате, например путем реализации подходящих средств управления из числа изложенных в настоящей Спецификации, а также в стандартах ИСО/МЭК 27002 и ИСО/МЭК 27018.

18.1.3 Права интеллектуальной собственности

См. средство управления, определяемое в пункте 18.1.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

18.1.4 Защита записей

См. средство управления, определяемое в пункте 18.1.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

18.1.5 Конфиденциальность и защита информации, позволяющей установить личность

См. средство управления, определяемое в пункте 18.1.4 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

18.1.6 Регуляторные положения, касающиеся средств управления с использованием шифрования

См. средство управления, определяемое в пункте 18.1.5 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

18.2 Анализ уровня информационной безопасности

18.2.1 Введение

См. задачу, изложенную в пункте 18.2 стандарта ИСО/МЭК 27002:2013.

18.2.1 Независимый анализ уровня информационной безопасности

См. средство управления, определяемое в пункте 18.2.1 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте. См. также приведенные ниже дополнительные руководящие указания.

Руководящие указания по реализации для защиты PII

В случаях когда проведение аудита силами отдельных заинтересованных сторон не представляется возможным или может быть сопряжено с повышенными рисками для безопасности, организации перед заключением договоров должны снабдить заинтересованные стороны независимым свидетельством того, что обеспечение информационной безопасности реализуется и осуществляется в соответствии с правилами и процедурами диспетчера PII. Соответствующий независимый аудит по выбору диспетчера PII, как правило, должен быть приемлемым для заинтересованных сторон методом проверки деятельности диспетчера по обработке PII при условии обеспечения достаточной прозрачности.

18.2.3 Соответствие требованиям политики и стандартов безопасности

См. средство управления, определяемое в пункте 18.2.2 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

18.2.4 Анализ соответствия техническим требованиям

См. средство управления, определяемое в пункте 18.2.3 стандарта ИСО/МЭК 27002, сопутствующие руководящие указания по его реализации и иную информацию в этом стандарте.

Приложение A

Расширенный комплекс средств управления для защиты PII

(Данное Приложение является неотъемлемой частью настоящей Рекомендации |Международного стандарта)

A.1 Общее

В настоящем Приложении излагаются новые задачи, средства управления и руководящие указания, которые образуют расширенный комплекс средств управления по реализации конкретных требований к защите PII.

Руководящие указания, приведенные в настоящей Спецификации, основываются на соответствующих положениях стандарта ISO 29100:2011 и предполагают, что эти положения уже реализованы.

В пункте A.1 излагается общая политика защиты PII, а последующие пункты отражают принципы обеспечения конфиденциальности, описываемые в ИСО/МЭК 29100.

A.2 Общая политика использования и защиты PII

Задача – предоставить руководящие директивы и обеспечить поддержку для защиты PII в соответствии с бизнес-требованиями, а также требованиями нормативно-правовых актов.

Средство управления

Организациям, участвующим в обработке PII, следует установить политику использования и защиты PII.

Руководящие указания по реализации для защиты PII

Политика информационной безопасности должна включать (в виде отдельной политики защиты конфиденциальности или дополнений к имеющейся политике) надлежащие заявления о готовности и обязательстве обеспечивать соблюдение применимого законодательства по защите PII, договорных требований и внутренней политики.

Политика защиты конфиденциальности и политика безопасности, будучи тесно связанными, могут, тем не менее, регулировать разные вопросы. Как в политике информационной безопасности, так и в политике защиты конфиденциальности должны рассматриваться вопросы конфиденциальности, целостности и доступности информации, а в политике защиты конфиденциальности, кроме того, – вопросы согласия и индивидуального доступа.

Руководящие указания по реализации структурных основ защиты конфиденциальности содержатся в стандарте ИСО/МЭК 29100. Политика защиты PII должна:

- соответствовать целям организации;
- прозрачным образом описывать сбор и обработку PII в организации;
- задавать структурные основы для постановки задач по защите PII;
- устанавливать правила принятия решений по вопросам защиты PII;
- устанавливать критерии принятия степени рисков в отношении защиты конфиденциальности (см. также пункт 6.3.1 стандарта ИСО/МЭК 29134);
- включать обязательство соблюдения применимых требований защиты конфиденциальности;
- включать обязательство, касающееся непрерывного совершенствования;
- быть доведена до сведения сотрудников организации;
- быть доступна для ознакомления заинтересованным лицам, которых она касается.

A.3 Согласие и выбор

A.3.1 Согласие

Задача – привлечь субъектов PII к активному участию в процессе принятия решений по обработке затрагивающей их PII на основе свободно выраженного осмысленного и информированного согласия (за исключением ограничений, установленных нормативно-правовыми актами).

Средство управления

Организациям следует предоставить в распоряжение субъектов PII необходимые средства для свободного выражения осмысленного, информированного и однозначного согласия на обработку PII, за исключением случаев, когда субъект PII не вправе отказать в таком согласии или когда применимое законодательство явным образом разрешает обработку PII без согласия ее субъекта.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) определять практически реализуемые способы получения согласия от субъектов PII, анализировать случаи, в которых выбранные способы становятся неприменимыми, и при необходимости определять вместо них другие способы, позволяющие заблаговременно получить согласие субъекта на обработку PII;

b) предоставлять субъектам PII, в случаях когда это практически осуществимо и целесообразно или требуется по закону, способы для заблаговременного выражения согласия на обработку PII (под обработкой подразумевается сбор, хранение, внесение изменений, извлечение, консультация, раскрытие, удаление идентифицирующих элементов, обезличивание, распространение или иное предоставление доступа, удаление или уничтожение PII);

c) в случаях когда согласие дается законным представителем (например, от имени несовершеннолетнего или недееспособного лица), хранить регистрационную запись согласия;

d) когда это необходимо, уведомлять субъектов PII обо всех случаях передачи PII третьим лицам и предоставлять субъектам PII надлежащие способы для выражения их согласия на такую передачу;

e) заблаговременно получать согласие субъектов PII на новые способы использования или раскрытия ранее собранной PII;

f) обеспечивать, чтобы согласие было информированным, полученным в условиях полной прозрачности в отношении целей обработки PII; обеспечить также, чтобы согласие давалось для конкретной цели;

g) обеспечивать осведомленность и получать согласие, например, посредством обновляемых публичных уведомлений;

h) предоставлять субъектам PII механизм для изменения пределов их согласия на обработку PII$; в случае изменения пределов согласия незамедлительно принимать вытекающие из этого меры и соответственно прекращать обработку либо изменять ее характер;

i) обеспечивать, чтобы согласие соответствовало всем применимым законодательным требованиям (в том числе, когда это необходимо, требованию явного согласия на обработку чувствительной PII);

j) в случаях когда это целесообразно, предусмотреть возможность дачи подразумеваемого согласия, когда субъекты PII четко уведомляются об обработке, и отсутствие возражений с их стороны может служить знаком их согласия;

k) заблаговременно уведомлять о всех операциях, касающихся обработки PII; и

l) в случаях когда это необходимо, проверять личность субъекта PII или его законного представителя, дающего согласие на обработку (для проверки следует запрашивать минимально необходимый объем информации, хранить которую следует столько,

сколько требуется для данной цели, а после исчезновения надобности безопасно удалить).

Сопутствующая информация для защиты PII

Если иное не диктуется применимым законодательством, организациям следует получать явное или подразумеваемое согласие на обработку PII. Предпочтительно получать явное согласие, но этот способ не всегда осуществим. Для получения явного согласия необходимо, чтобы субъекты PII некоторым своим позитивным действием подтверждали, что разрешают организациям собирать или использовать PII. В случаях когда согласие дается электронным способом, организации следует определить, достаточно ли будет однократного явного согласия или же необходимо двойное.

Механизм явного отказа состоит в том, что организация предполагает неявное согласие субъекта PII на обработку затрагивающей его PII, если он некоторым свои позитивным действием не заявит об ином.

Вывод о подразумеваемом согласии обычно делается исходя из действий или бездействия какого-то лица либо из конкретных обстоятельств таких действий или бездействия. Пример подразумеваемого согласия – покупатель сообщает адрес доставки интернет-магазину, который затем использует эту информацию строго для целей доставки приобретенных покупателем товаров.

Организациям следует реализовать практические способы получения отдельного согласия субъектов PII в случаях, когда запрашиваются национальные идентификационные номера (например, номер социальной страховки, гражданский регистрационный номер, номер паспорта).

Например, организации могут предлагать на выбор перечень из пунктов, по которым субъект PII может выразить согласие на контакт с ним по любой выбранной цели. В этом случае организациям следует разработать механизмы получения согласия так, чтобы их организационная деятельность в максимальной степени соответствовала выбору субъекта PII.

Согласие может даваться в электронной форме или на бумаге в зависимости от применяемых требований нормативно-правовых актов и практических соображений.

В случаях когда PII передается в другую организацию или поступает из другой организации, организациям следует предусмотреть процесс обновления своих регистрационных записей для приведения их в соответствие с изменениями содержимого и статуса согласия (например, изменением пределов согласия или отзывом) по воле субъектов PII, а также для того, чтобы такие обновления/изменения производились далее в организациях, совместно с которыми используется PII. Запрашивать у субъекта PII и совместно использовать с другими организациями следует лишь минимальный объем информации, необходимой для обеспечения правильного обновления соответствующих регистрационных записей. Организациям следует периодически пересматривать свои процессы, чтобы исключить обработку ненужной PII.

A.3.2 Выбор

Задача – предоставить субъектам PII, в случаях когда это целесообразно и осуществимо, возможность по своему выбору не разрешать обработку затрагивающей их PII, отказать в согласии, отозвать согласие или возразить против конкретного вида обработки, а также разъяснить субъекту PII последствия дачи согласия или отказа в согласии.

Средство управления

Организациям следует предоставить в распоряжение субъектов PII четкие, заметные, легко понятные, доступные и приемлемые в ценовом отношении механизмы выбора при запросе согласия на обработку затрагивающей их PII, за исключением случаев, когда субъект PII не вправе отказать в согласии или когда применимое законодательство явным образом разрешает обработку PII без согласия ее субъекта.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) обеспечить, чтобы субъекты PII могли заблаговременно сделать выбор в отношении обработки затрагивающей их PII;

b) не отказывать в услуге субъекту PII, не согласившемуся предоставить PII, которая не относится к оказанию этой услуги;

c) в случаях, предусмотренных применимыми нормативно-правовыми актами, определить практические способы, посредством которых субъекты PII смогут осуществить свое право на возражение против обработки затрагивающей их PII (например, по почте, электронной почте или по телефону);

d) подтверждать прием заявления о возражении в сроки, установленные применимым законодательством или определяемые политикой организации;

e) проанализировать случаи, в которых выбранные практические способы становятся неприменимыми, и при необходимости определить вместо них другие резервные способы, позволяющие субъектам PII продолжать осуществлять свое право на возражение;

f) обеспечивать классификацию, маркировку и хранение PII таким способом, который облегчает осуществление права на возражение; обеспечить также возможность для субъектов PII своевременно и безвозмездно осуществить свое право на возражение;

g) подтверждать идентичность субъекта PII или его законного представителя, заявляющего о возражении против обработки; для проверки следует запрашивать минимально необходимый объем информации, хранить которую следует столько, сколько требуется для данной цели, а после исчезновения надобности безопасно удалить;

h) в случае если для осуществления права на возражение требуются правовые основания, обеспечить, чтобы в такой ситуации субъекты PII предоставляли разумные основания для возражения, а при отказе в удовлетворении возражения – излагали подробные причины, по которым диспетчер PII не считает эти основания правомерными;

i) обеспечить, чтобы возражения, представленные субъектом PII, были доведены до сведения всех организаций, совместно с которыми используется PII, и чтобы эти организации действовали в соответствии со всеми обоснованными возражениями;

j) по возможности предоставить субъектам PII возможность возражать против определенных видов обработки PII, вместо того чтобы соглашаться или не соглашаться с обработкой в целом.

Сопутствующая информация для защиты PII

Во многих ситуациях, в зависимости от применимого законодательства, может не существовать необходимости или реальной возможности предоставлять механизм для осуществления выбора при сборе общедоступной информации. Например, нет нужды предоставлять механизм выбора субъектам PII, получая их имена и адреса из документа публичного характера или газеты.

A.4 Правомерность и характеристики целей

A.4.1 Правомерность целей

Задача – обеспечить соответствие целей обработки PII применимому законодательству и наличие допустимых правовых оснований.

Средство управления

Организациям следует принять надлежащие меры, чтобы обеспечить соответствие целей обработки PII применимому законодательству и наличие допустимых правовых оснований.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) определить, может ли предлагаемая обработка осуществляться на иных правовых основаниях, помимо согласия (например, обеспечение соблюдения законов, общественная безопасность, правовое обязательство или законные интересы диспетчера PII);

b) определить, действует ли в отношении предлагаемой обработки правовое основание (например, обеспечение соблюдения законов, общественная безопасность или правовое обязательство), в соответствии с которым субъекты PII не вправе отказать в обработке интересующей их PII;

ПРИМЕЧАНИЕ. – В случае международного сбора или обработки PII необходимость в получении согласия и надлежащие способы обработки могут зависеть от конкретной применяемой правовой структуры.

c) определить правовое основание, разрешающее обработку PII, – либо в целом, либо для работы конкретной программы или информационной системы; и

d) внедрить процедуры, обеспечивающие соответствие выполняемой обработки всем применимым регуляторным положениям и их интерпретации компетентными органами. При определении правомерности целей обработки следует учитывать ее общий контекст, включая характер отношений между диспетчером PII и субъектами PII, состояние научно-технического прогресса и изменения общественно-культурных установок.

Организациям следует разработать процедуры, исключающие обработку PII такими способами, которые потенциально или реально нарушают любого рода правовые обязательства, в том числе законодательные положения, общеправовые нормы или условия договоров.

Если в организации имеется трудовой совет или профсоюз, применимое законодательство может требовать проведения консультаций с такими органами при определении правомерности целей, когда в роли субъектов PII выступают сотрудники.

По вопросам полномочий на сбор PII в рамках любых программ или видов деятельности руководителям программ следует проконсультироваться с лицом, ответственным за защиту PII (иногда называемым CPO) или замещающим его лицом, а также с юристом. Полномочия на сбор PII следует документально зафиксировать.

A.4.2 Характеристики целей

Задача – определить цели, для которых собирается PII, не позднее времени ее сбора, и в дальнейшем ограничить ее использование только для этих целей.

Средство управления

Организациям следует сообщать субъекту PII о целях сбора и обработки PII, которая у него запрашивается. Такое информирование должно происходить до или во время сбора PII и до обработки PII в любых целях, не сообщенных предварительно субъекту PII.

Руководящие указания по реализации для защиты PII

Организациям следует информировать субъекта PII о целях сбора и обработки PII до того, как эта информация будет собрана или впервые использована для новой цели. Цели должны быть сформулированы четко, сообразно конкретным обстоятельствам, с достаточными пояснениями по поводу необходимости в обработке чувствительной PII.

Нередко в законодательстве дается явное разрешение на сбор и использование PII для определенных целей. В случаях когда законодательные формулировки имеют широкое определение и, следовательно, открыты для толкования, организациям следует проконсультироваться с руководителем службы обеспечения конфиденциальности информации (CPO) и юристом, чтобы удостовериться в наличии четкой связи между таким разрешением общего характера и конкретной целью сбора PII.

Определив конкретные цели, следует четко изложить их в документации о соответствии требованиям защиты конфиденциальности или в формах для сбора PII, используемых организациями. Кроме того, во избежание несанкционированного сбора или использования PII следует провести подготовку персонала, работающего с PII, по вопросам полномочий организации в отношении сбора PII.

Организациям следует:

a) определить состав PII, которая требуется исключительно для конкретных бизнес-процессов;

b) логически отделить PII, которая требуется для каждого процесса;

c) установить разные права доступа в соответствии с бизнес-процессами (включая начисление заработной платы, обработку заявлений на отпуск и продвижение по службе) и создать выделенную ИТ-среду для систем, в которых обрабатывается наиболее чувствительная PII; и

d) регулярно проверять эффективность разделения PII, а также отсутствие новых получателей и взаимосвязей.

A.5 Ограничение на сбор информации

Задача – ограничить сбор PII тем минимумом, который допускается применимым законодательством и строго необходим для указанных целей.

Средство управления

Организациям следует принять надлежащие меры, чтобы ограничить номенклатуру типов и объем собираемой PII тем минимумом, который необходим для заявленных целей (см. пункт A.8.1) и допускается применимыми нормативно-правовыми актами.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) ограничить сбор PII тем минимумом информации, который определен для заявленных целей (см. пункт A.8.1) и на сбор которого получено согласие субъекта PII;

b) не собирать чувствительную PII, если сбор такой информации не разрешен законодательством или на него не дано согласие; и

c) ограничить объем информации, собираемой косвенным путем у самих субъектов PII или через побочные каналы (например, блоги, системные файлы журналов и т. д.).

Организациям следует определить цели обработки PII, состав необходимой для этих целей PII и состав информации, в сборе которой нет необходимости, а также убедиться, что собирается только необходимая чувствительная информация.

Организациям следует тщательно продумать, какая именно PII необходима для достижения конкретной цели, прежде чем приступать к сбору этой информации. Не следует собирать PII беспорядочно.

Организациям следует регулярно пересматривать цели сбора PII, чтобы убедиться, что эти цели по-прежнему актуальны. Кроме того, организациям следует регулярно пересматривать состав собираемой PII, чтобы убедиться, что он по-прежнему представляет собой необходимый минимум для соответствующих целей.

Организациям не следует собирать чувствительную PII, например национальный идентификационный номер, если сбор такой информации не разрешен законодательством или на него не дано явное согласие.

Сопутствующая информация для защиты PII

В некоторых юрисдикциях отдельные категории PII (например, раса, политические взгляды, религиозные и другие убеждения, личные медицинские данные, сведения о половой жизни, сведения о судимостях по уголовным статьям и т. д.) могут определяться как чувствительные. Эти юрисдикции могут устанавливать ограничения на сбор или условия сбора такой PII, и организациям следует учитывать эти ограничения и условия, принимая решение о составе собираемой PII.

A.6 Минимизация объема данных

Задача – ограничить объем обрабатываемой PII тем минимумом, который строго необходим для осуществления правомерных интересов диспетчера PII, и предельно ограничить круг заинтересованных лиц, которым раскрывается PII.

Средство управления

Организациям следует принять надлежащие меры, чтобы ограничить объем обрабатываемой PII тем минимумом, который строго необходим для осуществления правомерных интересов диспетчера PII (например, перед организацией может стоять задача интенсифицировать или расширить свою бизнес-деятельность определенным способом, который обоснованно влечет рост объема обрабатываемой и хранимой информации).

Руководящие указания по реализации для защиты PII

Организациям следует:

a) обеспечить принятие принципа необходимости в информации, когда доступ предоставляется только к той PII, которая необходима для выполнения должностных обязанностей конкретного лица в рамках правомерной цели обработки PII;

b) при всякой возможности использовать или предлагать по умолчанию такие способы взаимодействия и транзакций, которые не позволяют установить личность субъекта PII;

c) ограничить возможности установления взаимосвязей между элементами собираемой PII;

d) провести первичную оценку PII, хранящейся в организации, а затем разработать график и в соответствии с ним регулярно пересматривать информацию с целью убедиться, что собирается только та PII, которая заявлена, и что собираемая PII по-прежнему необходима для достижения текущих бизнес-целей;

e) ограничить круг заинтересованных лиц, которым передаются электронные документы, содержащие PII, теми лицами, которым эти документы необходимы для выполнения своей работы;

f) определить, какую PII следует подвергнуть обезличиванию или удалению идентифицирующих элементов, исходя из контекста, формы хранения PII (например, поля базы данных или текстовые фрагменты) и выявленных рисков;

g) удалить идентифицирующие элементы из данных, которые этого требуют, исходя из формы их хранения (например, поля базы данных или текстовые фрагменты) и выявленных рисков;

h) удалить и уничтожить PII во всех случаях, когда истек срок действия обработки PII, отсутствуют правовые требования хранения PII или когда это целесообразно; и

i) определить, допустимо ли использование технологий усиления защиты конфиденциальности (PET), и если да, то каких.

Минимальный набор элементов PII, необходимых для поддержки того или иного бизнес-процесса организации, может представлять собой подмножество PII, которую организация вправе собирать.

Всю совокупность PII следует разделить на обязательную и необязательную к сбору. Организациям следует собирать только обязательную PII, которая необходима для оказания услуг, а на сбор необязательной PII получать явное согласие субъектов PII. Организациям не следует отказывать в оказании услуг субъекту PII, не согласившемуся предоставить необязательную PII.

Лицу, ответственному за защиту конфиденциальности, и юристу следует потребовать у руководителей программ обоснования в отношении предлагаемой обработки PII, чтобы убедиться, что к сбору предназначается тот минимум PII, который необходим для работы с информационной системой или осуществления деятельности в правомерных целях.

ПРИМЕЧАНИЕ 1. – Согласно определению в стандарте ИСО/МЭК 29100 обезличивание – это процесс, посредством которого PII необратимо изменяется таким образом, что субъект PII уже не может быть прямо или косвенно идентифицирован диспетчером PII, действующим как в одиночку, так и в сотрудничестве с любой другой стороной. Такой процесс неизбежно приводит к необратимой потере информации. В некоторых случаях поставленной цели можно достичь, просто удалив часть данных.

ПРИМЕЧАНИЕ 2. – Планируется, что описание методов удаления идентифицирующих элементов из данных с усовершенствованной защитой, которое следует использовать для определения и проектирования мер по удалению идентифицирующих элементов согласно принципам защиты конфиденциальности, изложенным в ИСО/МЭК 29100, станет предметом будущего международного стандарта. По общему правилу, чтобы установить, что процесс удаления идентифицирующих элементов соответствует требованиям законодательства,

операцию по удалению идентифицирующих элементов следует выполнять, например, путем удаления или обобщения атрибутов в совокупности с принятием эффективных организационных и технических мер.

ПРИМЕЧАНИЕ 3. – Когда PII обрабатывается для той или иной цели, объем такой информации следует ограничить необходимым для этой цели минимумом, не раскрывая лишнюю информацию о субъекте PII. Например, если для опроса по тематике дорожного движения требуется информация о географическом местоположении респондента, следует рассмотреть возможность регистрации информации о расположенных поблизости ориентирах вместо точного адреса.

ПРИМЕЧАНИЕ 4. – Зачастую в ходе анализа обезличенных данных возможно раскрытие личностей субъектов PII, когда множество выходных данных невелико. Поэтому рекомендуется блокировать выход, если количество регистрационных записей оказывается меньше некоторого порогового значения, например 10. Это пороговое значение следует определить по итогам тщательного анализа на основе модели распределения данных.

Организациям следует снижать риски в отношении конфиденциальности и обеспечения безопасности, по возможности минимизируя перечень хранимой PII. Организациям следует провести первоначальную оценку PII, хранящейся в организации, а затем проводить пересмотры их PII для проверки полноты, точности, актуальности и значимости этого стека данных.

Организациям следует также ограничить хранение PII тем минимумом, который необходим для надлежащего выполнения документально зафиксированных бизнес-целей организации. Организациям следует разработать и опубликовать график периодического пересмотра своих хранимых данных для корректировки данных первоначального анализа.

Проводя периодическую оценку, организации снижают свои риски, ограничивая сбор данных только заявленным объемом и обеспечивая постоянную значимость и необходимость собираемых данных.

A.7 Ограничение на использование, хранение и раскрытие информации

A.7.1 Ограничение на использование, хранение и раскрытие информации

Задача – ограничить использование и раскрытие PII конкретными, четко сформулированными правомерными целями и хранить PII не дольше, чем это необходимо для достижения заявленных целей или соблюдения требований применимого законодательства.

Средство управления

Организациям следует принять надлежащие меры, чтобы ограничить обработку PII установленными правомерными целями и хранить PII не дольше, чем это необходимо для достижения заявленных целей или соблюдения требований применимого законодательства.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) ограничить использование, хранение и раскрытие (в том числе передачу) PII тем объемом, который необходим для достижения конкретных, четко сформулированных правомерных целей; и

b) настроить свои информационные системы для регистрации даты сбора, создания и обновления PII, а также даты предстоящего удаления или архивирования PII согласно утвержденному графику хранения регистрационных записей.

Руководящие указания по реализации в части использования для защиты PII

Организациям следует:

a) заблокировать (то есть архивировать, защитить от изменений и исключить из дальнейшей обработки) PII в случае, если заявленные цели обработки этой информации утратили актуальность, но применимое законодательство требует дальнейшего хранения;

b) обеспечить безопасное удаление или уничтожение PII (включая оригиналы, копии и архивные записи) надлежащими методами;

c) использовать PII только для целей, согласованных с субъектом PII или сообщенных ему до или во время сбора этой информации, а при необходимости также получать согласие перед любой обработкой PII в случае новой цели;

d) ограничить сторонний доступ к организационным системам и хранящейся в них PII, предоставляя его в пределах того, что строго необходимо и формально разрешено; если такой доступ действительно необходим для осуществления деятельности, необходимо следовать надлежащим процедурам выдачи разрешения;

e) до выдачи разрешения на подключение сторонних систем к организационным системам убедиться, что в сторонних системах реализованы надлежащие меры защиты;

f) периодически пересматривать меры защиты, реализуемые третьими сторонами, чтобы убедиться, что эти меры по-прежнему отвечают требованиям организации к безопасности. Если по итогам такого пересмотра меры защиты признаются недостаточными, следует отключать системы третьих сторон до введения в действие надлежащих мер защиты;

g) реализовать надлежащий механизм аутентификации при доступе к PII через удаленные интерфейсы, обеспечив при этом обязательное ведение журналов доступа к PII; и

h) распространить уведомление в целях информирования общественности о любых изменениях в составе хранимой PII, сбор которой производится в процессе мониторинга безопасности.

Руководящие указания по реализации в части хранения для защиты PII

Возможны обстоятельства, когда в силу законодательных требований PII хранится дольше, чем это необходимо для указанных бизнес-целей. Организациям следует:

a) хранить PII в течение разрешенного срока только для заявленных целей или в соответствии с законодательными либо договорными требованиями и незамедлительно удалять PII по истечении этого срока;

b) в случае когда требуется более длительное хранение PII, чем это необходимо для указанных бизнес-целей, реализовать меры по защите PII, например удаление идентифицирующих элементов;

c) установить ограниченные сроки хранения PII, соответствующие целям обработки;

d) убедиться, что в информационной системе предусмотрен автоматический контроль истечения срока хранения;

e) обеспечить соблюдение оговоренных сроков хранения и удаление PII по истечении этих сроков;

f) разработать функциональную возможность для автоматизированного удаления PII по истечении срока хранения; такое удаление должно производиться немедленно или при первой практической возможности;

g) определить, какие идентифицирующие элементы следует подвергнуть удалению, исходя из контекста, формы хранения PII (например, поля базы данных или текстовые фрагменты) и выявленных рисков;

h) удалить идентифицирующие элементы из данных, которые этого требуют, исходя из формы их хранения (например, поля базы данных или текстовые фрагменты) и выявленных рисков; и

i) выбрать методы защиты PII (в том числе частичное удаление, хеширование, хеширование ключа и индексирование) на случай, если удалить идентифицирующие элементы из этих данных не представляется возможным.

Руководящие указания по реализации в части раскрытия для защиты PII

Организациям следует:

a) не раскрывать PII третьим сторонам без предварительного уведомления и согласия субъекта PII, если такое раскрытие не допускается применимым законодательством; уведомление и согласие субъекта PII могут не требоваться при раскрытии информации

лицам и структурам внутри организации, например сотрудникам, которым эта информации необходима; и

b) предусмотреть эффективные механизмы защиты в процессе передачи PII, включая шифрование и защиту целостности данных.

Затрагивающую сотрудников PII следует удалить (например, безопасно удалять или архивировать) в соответствии с применимыми нормативно-правовыми актами и установленной в организации политикой ликвидации, а также, когда это уместно, с согласия сотрудника.

A.7.2 Безопасное удаление временных файлов

Задача – предусмотреть технические меры по безопасному удалению временных файлов в течение установленного срока.

Средство управления

Временные файлы и документы, которые могут содержать PII, следует удалять в течение установленного и документально зафиксированного срока.

Руководящие указания по реализации для защиты PII

В ходе нормальной работы информационных систем возможно создание временных файлов, которые могут содержать PII. Эти файлы специфичны для конкретной системы и приложения; в частности, они могут представлять собой содержимое файловой системы с возможностью отката и временные файлы, связанные с обновлением баз данных и работой другого прикладного программного обеспечения. Надобность во временных файлах обычно отпадает после того, как завершится выполнение соответствующей задачи по обработке информации, но бывает, что такие файлы не удаляются автоматически. Срок использования временного файла не всегда предсказуем, но процедура "сборки мусора" должна обеспечивать выявление оставшихся временных файлов и определение промежутка времени, прошедшего с момента их последнего использования.

В информационных системах, обрабатывающих PII, следует реализовать процедуру периодической проверки, обеспечивающей удаление временных файлов, которые не используются более установленного срока.

A.7.3 Уведомление о раскрытии PII

Задача – обеспечить, чтобы обработчик PII уведомлял диспетчера PII о поступлении юридически обязательного запроса на раскрытие PII.

Средство управления

В договоре между обработчиком PII и диспетчером PII следует предусмотреть положение, обязывающее обработчика PII уведомлять диспетчера PII в соответствии с оговоренной процедурой и в оговоренный срок о поступлении юридически обязательного запроса на раскрытие PII от правоохранительных и других компетентных органов, если иное не запрещено законом.

Руководящие указания по реализации для защиты PII

Организациям следует принять меры (например, предусмотрев соответствующие положения в договоре), направленные на то, чтобы:

a) обработчики PII консультировались с соответствующим диспетчером PII перед принятием юридически обязательных запросов на раскрытие PII, если иное не запрещено законом; и

b) обработчики PII принимали все предусмотренные договором запросы на раскрытие PII с разрешения соответствующего диспетчера PII, если иное не запрещено законом.

A.7.4 Регистрация раскрытий PII

Задача – обеспечить регистрацию раскрытий PII третьим сторонам.

Средство управления

Раскрытия PII третьим сторонам следует регистрировать с указанием того, когда, кому, какая информация и с какой целью была раскрыта.

Руководящие указания по реализации для защиты PII

Раскрытие PII может происходить в ходе нормального режима работы. Такое раскрытие следует регистрировать. Следует также регистрировать любые факты раскрытия PII третьим сторонам, например раскрытия в ходе расследований на законных основаниях или внешнего аудита. При этом в регистрацию следует включать источник раскрытия и основание для полномочий, позволяющих осуществлять раскрытие.

A.7.5 Раскрытие информации об передаче обработки PII на субподряд

Задача – обязать обработчиков PII раскрывать диспетчеру PII любую информацию о привлечении субподрядчиков.

Средство управления

Следует обеспечить, чтобы обработчик PII заблаговременно раскрывал диспетчеру PII информацию о привлечении субподрядчиков.

Руководящие указания по реализации для защиты PII

В договоре между обработчиком PII и диспетчером PII следует предусмотреть положения о передаче обработки PII на субподряд. В договоре следует указать, что привлечение субподрядчиков допускается только с предварительного разрешения диспетчера PII. Обработчику PII следует заблаговременно информировать диспетчера PII о любых планируемых изменениях, связанных с субподрядом, с тем чтобы диспетчер PII имел возможность возразить против таких изменений или отозвать свое согласие.

Информация, подлежащая раскрытию, должна включать факт использования субподряда и названия субподрядчиков, но не подробности конкретного бизнеса. Кроме того, раскрываемая информация должна включать перечень стран, в которых субподрядчики могут обрабатывать данные, и способы, с помощью которых обработчик PII обязывает субподрядчиков соблюдать или превышать его собственные обязательства.

В случаях когда публичное раскрытие информации о субподрядчиках, судя по оценкам, неприемлемым образом повышает риск для безопасности, раскрывать информацию следует на условиях соглашения о неразглашении и/или по запросу обработчика PII. Обработчика PII следует уведомить о наличии информации о действующих субподрядчиках.

A.8 Точность и качество

Задача – обеспечить точность, полноту, актуальность, достаточность обрабатываемой PII и ее значимость для установленной цели.

Средство управления

Организациям следует принять соответствующие меры, чтобы обеспечить надлежащее качество PII, прямо или косвенно полученной от субъекта PII.

Руководящие указания по реализации для защиты PII

Под обеспечением качества данных понимается обеспечение адекватной точности, полноты, актуальности, достаточности обрабатываемой PII и ее значимости для установленной цели.

Организациям следует:

a) разработать процедуры сбора PII, способствующие обеспечению ее точности и качества;

b) вести сбор PII таким образом, чтобы можно было обнаружить любые изменения после выхода информации за пределы авторитетного источника;

c) в максимально возможной степени, которая достижима на практике при сборе или формировании PII, убедиться в точности, значимости, актуальности и полноте PII;

d) обеспечить надежность PII, полученной из иных источников, нежели субъект PII, до обработки этой информации;

e) в случаях когда это целесообразно, проверить надлежащими способами обоснованность и правильность запросов на исправление от субъекта PII перед внесением каких-либо изменений в PII;

f) периодически производить проверку на предмет использования неточной или устаревшей PII в программах или системах и при необходимости исправлять эту информацию; и

g) выдать руководящие указания по обеспечению максимальной точности, полноты, достаточности и значимости распространяемой информации. Организациям следует принимать разумные меры для проверки точности PII. Такие меры могут включать, например, правку и проверку адресов в процессе их сбора и ввода в информационные системы с использованием интерфейсов прикладного программирования (API) для автоматизированной проверки адресов.

В случаях когда PII имеет достаточно чувствительный характер (например, используется для ежегодного подтверждения дохода налогоплательщика в целях получения периодического пособия), организациям следует встроить в свои информационные системы механизмы для определения метода и периодичности обновления информации и разработать соответствующие процедуры.

Чтобы свести к минимуму потенциальные неточности в данных, по возможности следует реализовать ввод PII в информационные системы самим субъектом PII, без переписывания данных другим лицом. Если же без переписывания PII не обойтись, то организациям следует рассмотреть возможность такой схемы, при которой субъект PII мог бы проверить транскрибированную информацию. Это помогает исправлять ошибки прежде, чем обработка неточной PII сможет нанести какой-либо последующий ущерб.

Сопутствующая информация для защиты PII

Виды мер, которые могут приниматься для обеспечения качества данных, могут зависеть от характера и контекста PII, а также способов ее получения и использования. Чем чувствительней PII, тем более обстоятельными должны быть меры по проверке точности этой информации. Для проверки PII, полученной из иных источников, нежели субъекты PII или их законные представители, могут потребоваться дополнительные меры.

A.9 Открытость, прозрачность и уведомление

A.9.1 Уведомление о защите конфиденциальности

Задача – предоставить достаточно подробные, написанные простым языком и вполне доступные уведомления о защите конфиденциальности.

Средство управления

Организациям следует принять надлежащие меры, чтобы уведомить субъектов PII о целях обработки PII.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) оперативно уведомлять субъектов PII относительно:

1) своей деятельности, оказывающей влияние на защиту конфиденциальности, включая, среди прочего, сбор, использование, совместное использование, защиту и безопасное удаление PII;

2) своих полномочий по сбору PII;

3) наличия или отсутствия у субъектов PII права выбора, касающегося способов использования PII организацией и последствий использования или неиспользования такого выбора;

4) возможности возражений против обработки PII;

b) предусмотреть механизмы уведомления и механизмы получения согласия, соответствующие эксплуатационным потребностям организации;

c) пересматривать свои уведомления для отражения изменений в практике или политике организации, затрагивающих PII, или изменений в ее деятельности, влияющих на защиту конфиденциальности, до введения в действие таких изменений или при первой практической возможности после этого;

d) обеспечить полноту уведомления и его соответствие целевой аудитории, исходя из характера PII, практических способов подачи уведомления и характера отношений между диспетчером PII и субъектом PII;

e) представлять информацию в ясном виде, чтобы она была понятна лицам, не знакомым с информационными технологиями, интернетом или юридическим жаргоном;

f) обеспечить, чтобы уведомление предоставлялось до или во время сбора PII;

g) исключить возможность сбора PII без уведомления;

h) предусмотреть альтернативные решения на случай, если выбранные практические способы станут неприменимыми;

i) по возможности предусмотреть способы, позволяющие показать, что уведомление было произведено;

j) в случаях когда уведомление по вопросам конфиденциальности предоставляется с помощью физических средств, разместить эту информацию на предупредительном знаке, который должен быть виден субъектам PII, или потребовать расписки на уведомлении или документе; и

k) предусмотреть политику предоставления меток и знаков, необходимых для информирования субъектов PII об использовании соответствующих технических средств (например, систем охранного видеонаблюдения (CCTV), сетей Wi-Fi и меток радиочастотной идентификации (RFID)).

По мере возможности следует разместить уведомление на видном месте – там, где производится сбор информации (например, на веб-сайте организации или в помещении), не вынуждая субъекта PII специально просить об этом.

A.9.2 Открытость и прозрачность

Задача – предоставить субъектам PII в легкодоступном виде и четком изложении информацию об используемых диспетчером PII положениях, касающихся политики, процедур и практики обращения с PII.

Средство управления

Организациям следует принять надлежащие меры в целях предоставления субъектам PII адекватной информации о принятых в организации политике, процедурах и практике обращения с PII.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) предоставлять субъектам PII в легкодоступном виде и четком изложении информацию об используемых диспетчером PII положениях, касающихся политики, процедур и практики обращения с PII;

b) уведомлять субъектов PII о предлагаемых диспетчером PII возможностях и способах для целей ограничения обработки затрагивающей их информации, а также для доступа к ней, ее исправления и удаления.

Кроме того, организации должны предоставить следующую информацию:

a) состав PII, собираемой организацией, и цели, для которых эта информация собирается;

b) способы использования PII внутри организации;

c) используется ли PII организацией совместно с внешними объектами, категории этих объектов и цели такого совместного использования;

d) имеется ли у субъектов PII возможность дать согласие на конкретные способы использования или совместного использования PII и какими способами можно выразить такое согласие;

e) сроки хранения PII;

f) осуществляет ли организация перепродажу или перенаправление данных для обработки в сторонние аналитические организации и каковы связанные с этим риски для PII;

g) как субъекты PII могут получить доступ к затрагивающей их PII для внесения поправок или корректировок в случаях, когда это целесообразно;

h) соответствующие сведения о том, как будет защищаться PII;

i) сведения об обеспечении доступа субъекта PII к информации о деятельности организации по вопросам конфиденциальности и о способах связи с руководителем службы обеспечения конфиденциальности информации;

j) по соответствующему запросу сведения об утечках конфиденциальной информации, которые привели или могли привести к нарушению конфиденциальности подателя запроса о PII, а также о действиях, которые может предпринять податель запроса для снижения дополнительных рисков, обусловленных утечкой.

Организациям следует использовать также разные механизмы для публичного уведомления о своей практике в отношении защиты конфиденциальности, включая, среди прочего, отчет PIA, отчеты о защите конфиденциальности, общедоступные веб-страницы, рассылки электронной почты, блоги и периодические публикации (например, ежеквартальные новостные бюллетени). Организациям следует задействовать также публичные адреса электронной почты и/или телефонные линии, позволяющие пользователям иметь обратную связь или напрямую обращаться в службы защиты конфиденциальности по практическим вопросам обеспечения конфиденциальности.

A.10 Участие и доступ субъектов PII

A.10.1 Доступ субъектов PII

Задача – предоставить субъектам PII возможность доступа к затрагивающей их PII, проверить эту информацию и оспорить ее точность и полноту.

Средство управления

Организациям следует принять надлежащие меры, чтобы предоставить субъектам PII возможность доступа к затрагивающей их PII, корректировки этой информации и/или ее удаления.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) определить практические способы, посредством которых субъекты PII смогут осуществить свое право на доступ (в случаях, когда это разрешено применимым законодательством). При этом должна быть возможность осуществить такое право своевременно, в понятной и доступной для субъекта PII форме и способом, аналогичным тому, который первоначально использовался для сбора PII (например, по обычной или электронной почте);

b) проанализировать случаи, в которых выбранные практические способы становятся неприменимыми, и при необходимости определить вместо них резервное решение;

c) предоставить субъектам PII возможность доступа к затрагивающей их PII в том виде, в котором она хранится в организации, для целей проверки этой информации и подачи запроса на ее корректировку в случае необходимости;

d) по мере возможности давать ответы в той же форме, в которой делался запрос (например, если запрос поступил обычной почтой, ответ следует также направить по обычной почте);

e) публиковать правила и нормативные положения, регулирующие возможные способы запросить доступ субъектов PII к регистрационным записям, хранящимся в системах организации;

f) предоставлять субъектам PII возможность прямо или косвенно оспаривать точность и полноту PII, а также вносить поправки, корректировать или удалять эту информацию в зависимости от того, что уместно и возможно в конкретном контексте;

g) установить процедуры, позволяющие субъектам PII просто, быстро и эффективно осуществлять эти права без необоснованных задержек (например, ответы следует давать в соответствии с применимыми нормативно-правовыми актами или политикой организации) или расходов;

h) установить процесс информирования субъектов PII, подавших запросы, о статусе их запросов и необходимой обработке (например, по обычной или электронной почте, с уведомлением о получении запроса и о дате, к которой можно ожидать ответ); при работе с физическими архивами срок ответа на запрос может быть продлен на некоторое время, если диспетчер PII уведомит подавшего запрос субъекта PII о временных рамках обработки запроса и укажет разумный срок ответа;

i) в максимально возможной степени, разрешенной законодательством, обеспечивать, чтобы субъект PII всегда имел возможность осуществлять свое право доступа;

j) обеспечивать, чтобы доступ к PII могло получить только то лицо, которого затрагивает эта информация, или его законный представитель; для этого может потребоваться надлежащая идентификация и аутентификация лиц, запрашивающих доступ; требования к такой идентификации и аутентификации могут устанавливаться применимыми нормативно-правовыми актами;

k) в случаях, требующих идентификации и аутентификации лиц, запрашивающих доступ, если иное не предписывается применимыми нормативно-правовыми актами, определить надлежащую форму идентификации и аутентификации; при этом организации для целей корректной идентификации должны запрашивать только необходимый минимум информации, которую следует надежно защищать и хранить до тех пор, пока это необходимо;

l) обеспечивать, чтобы PII направлялась только соответствующему субъекту PII и пересылалась безопасным способом;

m) обеспечивать предоставление субъектам PII всей информации, которую они могут запросить, с одновременной защитой PII, затрагивающей других субъектов;

n) сообщать в уведомлении о защите конфиденциальности, предполагается ли взимание каких-либо сборов за доступ, которые могут быть разрешены законом в некоторых юрисдикциях; и

o) требовать от обработчиков PII оказания поддержки диспетчеру PII в упрощенном осуществлении права субъектов PII на доступ к затрагивающим их данным, а также на исправление и удаление этих данных.

Право доступа обеспечивает субъектам PII возможность узнать, какая затрагивающая их PII хранится в системах регистрационных записей организации. При этом предполагается своевременный, упрощенный и недорогой доступ к регистрационным данным. Процессы, обеспечивающие доступ к учетным записям в организации, могут различаться в зависимости от имеющихся ресурсов, законодательных требований и других факторов.

A.10.2 Корректировка и участие

Задача – обеспечить уведомление обработчиков PII и третьих сторон, которым были раскрыты персональные данные, о любых поправках, корректировках или удалении PII, находящейся в их распоряжении.

Средства управления

Если это не запрещено применимыми нормативно-правовыми актами, организациям следует принять надлежащие меры, чтобы субъекты PII имели возможность вносить поправки, корректировать или удалять PII, которая хранится в организациях. Кроме того, организациям следует предусмотреть механизм, позволяющий уведомлять о всех поправках, корректировках или удалении PII обработчиков PII и, по мере возможности, третьи стороны, которым была раскрыта PII.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) обеспечивать, чтобы субъект PII всегда имел возможность осуществлять свое право на корректировку;

b) анализировать случаи, в которых выбранные практические способы становятся неприменимыми, и при необходимости определить вместо них резервные решения;

c) в максимально возможной степени, разрешенной применимыми нормативно-правовыми актами, обеспечивать, чтобы субъект PII всегда имел возможность осуществлять свое право на корректировку;

d) обеспечивать точность запрашиваемых корректировок;

e) обеспечивать, чтобы субъектам PII, подающим запросы, направлялись подтверждения о получении запросов;

f) обеспечивать информирование третьих сторон, которым могла быть передана PII, о произведенных корректировках; и

g) предоставлять субъектам PII доступ только к той PII, которую им необходимо корректировать, исправлять или удалять.

A.10.3 Управление жалобами

Задача – ввести процедуры эффективной обработки жалоб в организации и внесения исправлений, предназначенные для использования субъектами PII.

Средства управления

Организациям следует принять надлежащие меры для эффективной обработки жалоб, поступающих от субъектов PII.

Руководящие указания по реализации для защиты PII

Организациям следует реализовать процесс управления жалобами и поддерживать работу контактного пункта для приема жалоб, замечаний и вопросов от субъектов PII о принятых в организации практиках защиты конфиденциальности, а также для ответа на эти жалобы, замечания и вопросы.

Организациям при этом следует предусмотреть механизмы приема жалоб, которые легко доступны субъектам PII, обеспечивают предоставление всей информации, необходимой для успешной подачи жалоб (в том числе контактной информации руководителя службы обеспечения конфиденциальности информации (CPO) или другого официального лица, в обязанности которого входит прием жалоб), и просты в использовании.

Процессы управления жалобами в организации должны также предусматривать механизмы отслеживания, обеспечивающие рассмотрение всех поступивших жалоб и надлежащее реагирование на них в должные сроки. Наконец, в рамках управления жалобами следует предусмотреть принятие корректирующих мер по результатам обработки жалоб.

Сопутствующая информация для защиты PII

Жалобы, замечания и вопросы субъектов PII могут служить ценным источником внешнего воздействия, которое в конечном счете позволяет совершенствовать рабочие модели, применение новых технологий, практику обработки данных, а также методы защиты конфиденциальности и обеспечения безопасности.

A.11 Подотчетность

A.11.1 Управление

Задача – наладить эффективное управление для целей обработки PII.

Средство управления

Организациям следует принять надлежащие меры для налаживания эффективного управления для целей обработки PII.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) назначить лицо, ответственное за разработку, реализацию и ведение в масштабах организации программы управления и защиты конфиденциальности, направленной на обеспечение соответствия всем применимым нормативно-правовым актам, касающимся обработки PII с помощью программ и информационных систем; это лицо может быть назначено на роль CPO либо данная ответственность может быть возложена на специального члена совета директоров при поддержке специально выделенного персонала, который может привлекаться на началах субподряда;

b) обеспечить наличие у назначенного лица необходимой квалификации для надзора за обработкой PII;

c) обеспечить участие назначенного лица в решении всех вопросов, связанных с защитой PII, и возможность для него своевременно напрямую отчитываться перед высшим руководством;

d) обеспечить назначенное лицо надлежащим персоналом, рабочими помещениями, оборудованием и другими ресурсами, необходимыми для выполнения поставленных перед ним задач;

e) предусмотреть процесс мониторинга законодательства о защите конфиденциальности и соответствующей политики на предмет изменений, влияющих на программу защиты PII;

f) разработать, распространить и реализовать эксплуатационные принципы и процедуры защиты PII, с помощью которых будут регулироваться средства управления для защиты PII и обеспечения безопасности применительно к программам, информационным системам или технологиям, имеющим отношение к работе с PII;

g) периодически обновлять план, принципы и процедуры защиты PII; и

h) осуществлять периодический мониторинг показателей деятельности организации в области защиты PII. Представитель высшего руководства или член совета директоров должен управлять этим процессом с учетом таких аспектов, как количественные показатели, риски и утечки; хотя такой мониторинг может осуществляться и по необходимости, но рекомендуется сделать его регулярным без необходимости в каких-либо побудительных причинах.

A.11.2 Оценка воздействия на защиту конфиденциальности

Задача – установить процесс оценки воздействия на защиту конфиденциальности и проводить такую оценку воздействия по мере необходимости.

Средство управления

Если та или иная организация обрабатывает PII, то этой организации следует установить процедуры, необходимые для проведения PIA.

Руководящие указания по реализации для защиты PII

Оценка рисков для защиты конфиденциальности проводится обычно организациями, которые серьезно относятся к своей ответственности и надлежащим образом выстраивают взаимоотношения с субъектами PII. В некоторых юрисдикциях PIA может быть необходимой в целях соблюдения требований нормативно-правовых актов. Источником руководящих указаний по проведению PIA может служить стандарт ИСО/МЭК 29134.

При оценке рисков для защиты конфиденциальности организациям следует принимать во внимание активы, угрозы, уязвимости и меры защиты (существующие и предлагаемые). Организациям следует документально фиксировать:

a) результаты PIA, включая, в том числе, обрабатываемую PII;

b) выявленные риски для защиты конфиденциальности; и

c) предлагаемые меры по уменьшению рисков.

A.11.3 Требования защиты конфиденциальности, адресованные подрядчикам и обработчикам PII

Задача – посредством договорных требований или другими способами (например, с помощью обязательной внутренней политики) побудить стороннего получателя PII обеспечить как минимум эквивалентный уровень защиты PII.

Средство управления

Организациям следует принять надлежащие меры, чтобы обязать подрядчиков и обработчиков PII обеспечить достаточные уровни защиты PII.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) документально зафиксировать обязательные требования к защите PII в соглашении об уровне обслуживания, заключаемом с обработчиками PII;

b) отслеживать и проверять соблюдение этих требований подрядчиками;

c) установить распределение ролей и ответственности в сфере защиты PII для подрядчиков и обработчиков PII;

d) установить в договоре с обработчиком PII предмет и временные рамки оказываемой услуги, объемы, способы и цели обработки PII, а также типы обрабатываемой PII;

e) установить условия, при которых обработчик PII обязан возвратить или безопасно удалить PII по завершении обслуживания, после прекращения действия соответствующего соглашения или на иных основаниях по запросу диспетчера PII;

f) предусмотреть в договоре положение о конфиденциальности, имеющее обязательную силу в отношении как поставщика услуг, так и всех его сотрудников, которые могут иметь доступ к PII;

g) исключить передачу PII от поставщика услуг третьим сторонам даже в целях ее сохранения, если это специально не предусмотрено в договоре;

h) уточнить обязанности поставщика услуг по уведомлению диспетчера PII о любой утечке данных, оказывающей влияние на защиту конфиденциальности;

i) зафиксировать в договоре обязанность поставщика услуг уведомлять диспетчера PII о любых значимых изменениях в своих услугах, например о реализации дополнительных функций; и

j) документально зафиксировать и довести до сведения адресатов все принципы, процедуры и практические методы, связанные с защитой PII.

Организациям следует проконсультироваться с юристом, CPO и специалистами по заключению договоров о применимых законах, директивах, принципах или регуляторных положениях, которые могут повлиять на реализацию этого средства управления.

ПРИМЕЧАНИЕ. Реализуются также дополнительные руководящие указания, изложенные в пункте 15.1.2.

Сопутствующая информация для защиты PII

К подрядчикам и обработчикам PII могут относиться, среди прочего, бюро обслуживания, поставщики информации, обработчики информации и другие организации, предлагающие услуги по разработке информационных систем, услуги информационных технологий и другие услуги сторонних организаций.

A.11.4 Мониторинг и аудит в целях защиты конфиденциальности

Задача – осуществлять мониторинг и аудит средств управления для защиты PII и эффективности внутренней политики защиты PII.

Средство управления

Организациям следует принять надлежащие меры для периодического мониторинга и аудита средств управления для защиты конфиденциальности и эффективности внутренней политики по защите конфиденциальности.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) осуществлять регулярный мониторинг и аудит деятельности по обработке PII (особенно информации, содержащей чувствительную PII), чтобы обеспечить соответствие этой деятельности применимым нормативно-правовым и договорным требованиям;

b) осуществлять регулярный мониторинг и аудит средств управления и принципов защиты PII, чтобы обеспечить их соответствие применимым нормативно-правовым и договорным требованиям;

c) обеспечивать проведение аудитов квалифицированными независимыми структурами (внутренними или внешними по отношению к организации); и

d) в случае проведения аудитов с использованием внутренних ресурсов периодически привлекать внешнюю организацию для проведения независимого аудита.

A.11.5 Информирование и подготовка в области защиты PII

Задача – обеспечить надлежащую подготовку и информирование в области защиты PII для персонала диспетчера PII, которому будет предоставляться доступ к PII.

Средство управления

Организациям следует принять соответствующие меры для обеспечения надлежащей подготовки персонала диспетчера PII.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) реализовывать и оказывать поддержку комплексной стратегии подготовки и информирования, направленной на разъяснение персоналу его ответственности в области защиты PII и соответствующих процедур;

b) создавать механизмы информирования персонала, выполняющего обязанности по защите PII, об изменениях обстановки в регуляторной, договорной и технологической

сферах, которые могут повлиять на соответствие организации требованиям защиты конфиденциальности;

c) проводить базовую и специализированную ролевую подготовку персонала в области защиты PII на регулярной основе (например, ежегодно) или по мере необходимости (например, по итогам какого-либо инцидента). Это особенно важно для тех видов деятельности, в рамках которых обработка PII происходит нечасто; и

d) обеспечивать периодическое подтверждение персоналом (на бумаге или в электронной форме) принятия ответственности за соблюдение требований защиты PII.

A.11.6 Отчетность о защите PII

Задача – составлять, распространять и обновлять отчеты о защите PII.

Средство управления

Организациям следует составлять и в зависимости от ситуации распространять отчеты (например, об утечках, расследованиях, аудитах), адресованные высшему руководству и другому персоналу, в обязанности которого входит мониторинг защиты PII, с целью продемонстрировать подотчетность в рамках мандатов по конкретным программам защиты PII согласно действующим нормативно-правовым требованиям.

Руководящие указания по реализации для защиты PII

Посредством внешней и внутренней отчетности о защите PII организациям следует обеспечивать подотчетность и прозрачность своей деятельности по защите PII. Отчетность также помогает организациям отслеживать свой прогресс в обеспечении соответствия требованиям по защите PII и реализации средств управления для защиты PII, сравнивать показатели деятельности различных структур внутри организации, выявлять уязвимые места и пробелы в политике и ее реализации, а также определять модели достижения успеха.

A.12 Информационная безопасность

Задача – обеспечить надлежащую защиту PII в соответствии с результатами оценки рисков.

Средство управления

Хранящуюся в организации PII следует защищать путем применения надлежащих организационно-технических мер в соответствии с результатами оценки рисков угроз или PIA.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) защищать PII путем надлежащих средств управления на эксплуатационном, функциональном и стратегическом уровнях, чтобы обеспечить целостность, конфиденциальность и доступность PII, а также уберечь эту информацию от рисков несанкционированного доступа, уничтожения, использования, модификации, раскрытия или потери на протяжении всего ее жизненного цикла;

b) выбирать обработчиков PII и заключать с ними договоры, содержащие достаточные гарантии в отношении организационных, физических и технических средств управления для обработки PII и обеспечения соответствия требованиям, предъявляемым к этим средствам управления;

c) при определении средств управления безопасностью исходить из применимых законодательных требований, стандартов безопасности, результатов систематической оценки рисков для безопасности, проводимой в соответствии со стандартом ISO 31000, а также результатов анализа экономической эффективности;

d) ограничить доступ к PII теми лицами, которым такой доступ необходим для выполнения служебных обязанностей, и ограничить доступ этих лиц только той PII, которая необходима им для выполнения служебных обязанностей;

e) принимать меры по противодействию рискам и по устранению уязвимостей, выявленных в ходе оценки рисков для защиты конфиденциальности и в процессах аудита; и

f) осуществлять периодический пересмотр средств управления и переоценку рисков в рамках непрерывного процесса управления рисками для безопасности.

Иногда требования безопасности предписываются определенными законами о защите конфиденциальных данных, и такие требования следует сообщать функциональному подразделению обеспечения безопасности данных, в задачи которого входит их реализация.

При проектировании и реализации средств управления безопасностью следует соблюдать должную осмотрительность.

A.13 Соответствие требованиям защиты конфиденциальности

A.13.1 Соответствие требованиям

Задача – исключить нарушения обязательств, установленных нормативно-правовыми актами, договорами или политикой защиты конфиденциальности, а также прочих требований защиты конфиденциальности.

Средство управления

Организациям следует принять надлежащие меры, с тем чтобы обработка PII соответствовала установленным требованиям.

Руководящие указания по реализации для защиты PII

Организациям следует:

a) ежегодно представлять отчет с описанием имеющихся рисков, информацией об уровне соответствия требованиям и перечнем подлежащих выполнению действий; и

b) соблюдать четко определенные процессы реагирования на утечки, которые в ряде юрисдикций могут среди прочего включать требование об уведомлении субъектов PII и компетентных органов (например, органов по защите данных).

A.13.2 Ограничения на трансграничную передачу данных в некоторых юрисдикциях

Задача – защитить PII при трансграничной передаче.

Средство управления

Организациям следует принять надлежащие меры, чтобы обеспечить соответствие определенным требованиям при трансграничной передаче PII.

Руководящие указания по реализации для защиты PII

Когда возникает необходимость передать PII в другую страну, регуляторные положения некоторых юрисдикций по защите конфиденциальных данных могут налагать одно или несколько ограничений из следующего перечня:

a) необходимость уведомления органа по защите данных;

b) необходимость получения разрешения органа по защите данных, особенно если данные являются чувствительными;

c) необходимость соблюдения должной осмотрительности, чтобы обеспечить защиту передаваемой через границу PII на уровне, эквивалентном тому, который требуется в стране-источнике; и

d) реализация конкретных инструментов передачи данных, таких как типовые договорные положения или обязательные корпоративные правила (BCR).

Организациям следует принять надлежащие меры для проверки применимости конкретных ограничений к любой запланированной передаче данных и обеспечить соблюдение этих ограничений, прежде чем приступать к передаче.

Библиография

– BSI 10012, Specification for a personal information management system

– European Commission, Evaluation report on the data retention directive (Directive 2006/24/EC), 2011.

– ISO/IEC 27000:2016, Information technology – Security techniques – Information security management systems – Overview and vocabulary

– ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.

– ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management.

– ISO/IEC 27009, Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements.

– ISO/IEC 27018, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

– ISO/IEC 29134, Information technology – Security techniques – Guidelines for privacy impact assessment.

– База данных МЭК Electropedia, доступна (по состоянию на 6 июля 2017 г.) по адресу: http://www.electropedia.org/.

– Онлайновая навигационная платформа ИСО, доступна (по состоянию на 6 июля 2017 г.) по адресу: http://www.iso.org/obp.

– База данных "Термины и определения МСЭ", доступна (по состоянию на 7 июля 2017 г.) по адресу: http://www.itu.int/ITU-R/go/terminology-database.

– KCS, Personal information management system, December, 2011.

– NIST Special Publication 800-53 Appendix J, Security and privacy controls for federal information systems and organizations, July, 2011.

– NIST Special Publication 800-122, Guide to protecting the confidentiality of personally identifiable information (PII), April 2010.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета, а также экономические и политические вопросы, связанные с международными услугами в области электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2017 г.