ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59407— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Базовая архитектура защиты персональных данных

(ISO/IEC 29101:2018, NEQ)

Издание официальное

Москва
Стандартинформ
2021

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО «ИАВЦ») и Акционерным обществом «Аладдин Р.Д.» (АО «Аладдин Р.Д.»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. № 415-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта ИСО/МЭК 29101:2018 «Информационные технологии. Методы и средства обеспечения безопасности. Архитектура обеспечения приватности» (ISO/IEC 29101:2018 «Information technology — Security techniques — Privacy architecture framework», NEQ).

ИСО/МЭК 29101 разработан подкомитетом ПК 27 «Методы и средства обеспечения безопасности ИТ» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК)

5 ВВЕДЕН ВПЕРВЫЕ

6 Федеральное агентство по техническому регулированию и метрологии не несет ответственности за патентную чистоту настоящего стандарта. Патентообладатель может заявить о своих правах и направить в национальный орган по стандартизации аргументированное предложение о внесении в настоящий стандарт поправки для указания информации о наличии в стандарте объектов патентного права и патентообладателе

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

© Стандартинформ, оформление, 2021

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 2
3.1 Термины и определения 2
3.2 Сокращения 3
4 Общий обзор базовой архитектуры защиты персональных данных 3
4.1 Элементы архитектуры 3
4.2 Взаимосвязь с системой управления 4
5 Участники обработки персональных данных 4
5.1 Общие положения 4
5.2 Этапы жизненного цикла персональных данных при обработке 5
6 Значимые вопросы 7
6.1 Общие положения 7
6.2 Принципы обеспечения безопасности персональных данных 7
6.3 Требования защиты персональных данных 7
7 Архитектурные представления 8
7.1 Общие положения 8
7.2 Представление с точки зрения компонентов 8
7.3 Представление с точки зрения действующих субъектов (сторон) 19
7.4 Представление с точки зрения взаимодействия 22
Приложение А (справочное) Примеры значимых вопросов, связанных с защитой персональных данных 25
Приложение Б (справочное) Система агрегирования персональных данных с безопасными вычислениями 29
Приложение В (справочное) Архитектура системы управления идентификационными данными и управления доступом, способствующая защите персональных данных 34
Библиография 39

Введение

Настоящий стандарт предоставляет описания высокоуровневой базовой архитектуры и соответствующих мер защиты персональных данных в информационных системах персональных данных.

Описанная в настоящем стандарте архитектура защиты персональных данных:

- предоставляет последовательный высокоуровневый подход к реализации мер защиты при обработке персональных данных с использованием средств автоматизации;
- предоставляет руководство по планированию, проектированию и построению архитектур информационных систем персональных данных, которые обеспечивают защиту персональных данных путем контроля за их обработкой, доступом и передачей;
- показывает, как технологии, обеспечивающие конфиденциальность персональных данных действующих субъектов персональных данных, могут использоваться в качестве мер защиты.

Настоящий стандарт учитывает основные положения нормативных правовых актов Российской Федерации.

Положения настоящего стандарта не исключают применение криптографических методов (алгоритмов) при обеспечении безопасности персональных данных, в частности их шифрование, но не устанавливают требования по их реализации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Базовая архитектура защиты персональных данных

Information technology. Security techniques. Personal data protection architecture framework

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт содержит описание базовой архитектуры защиты персональных данных, которая:

- определяет значимые вопросы, касающиеся информационных систем персональных данных;
- предоставляет перечень компонентов при реализации таких систем;
- предоставляет базовые архитектурные решения, рассматриваемые в контексте данных компонентов.

Настоящий стандарт применим для организаций, участвующих в определении, приобретении, разработке архитектуры, проектировании, тестировании, поддержке, администрировании и эксплуатации информационных систем персональных данных.

Основное внимание в настоящем стандарте уделено информационным системам персональных данных, предназначенным для взаимодействия с субъектами персональных данных.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 50922 Защита информации. Основные термины и определения

ГОСТ Р 57100—2016/ISO/IEC/IEEE 42010:2011 Системная и программная инженерия. Описание архитектуры

ГОСТ Р 58833 Защита информации. Идентификация и аутентификация. Основные положения

ГОСТ Р 59382 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 50922 и ГОСТ 58833, а также следующие термины с соответствующими определениями:

3.1.1 **безопасность персональных данных:** Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

3.1.2

информационная система персональных данных: Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

[[1], статья 3, пункт 10]

3.1.3 **конфиденциальность персональных данных:** Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

3.1.4 **нарушитель безопасности персональных данных:** Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

3.1.5

обезличивание персональных данных: Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

[[1], статья 3, пункт 9]

3.1.6

обработка персональных данных: Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

[[1], статья 3, пункт 3]

3.1.7

оператор: Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

[[1], статья 3, пункт 2]

3.1.8 **персональные данные:** Любая информация, относящаяся к прямо или косвенно определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Примечания

1 Адаптировано из [1], статья 3.

2 Персональными данными являются, например, фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация физического лица.

3.1.9

предоставление персональных данных: Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
[[1], статья 3, пункт 6]

3.1.10 **распространение персональных данных:** Действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

3.1.11 **угрозы безопасности персональных данных:** Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

3.1.12 **уничтожение персональных данных:** Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3.2 Сокращения

В настоящем стандарте применены следующие сокращения:

ИСПДн — информационная система персональных данных;

ПДн — персональные данные.

4 Общий обзор базовой архитектуры защиты персональных данных

4.1 Элементы архитектуры

Представленная в настоящем стандарте базовая архитектура защиты ПДн предназначена для использования в качестве технического руководства для разработчиков ИСПДн. Настоящий стандарт не устанавливает требования для политик защиты ПДн; предполагается, что политики приняты и что в рамках ИСПДн определены требования защиты ПДн, а также реализованы соответствующие меры защиты ПДн.

Данная базовая архитектура направлена на защиту ПДн. Поскольку защита ПДн является целью обеспечения безопасности информации, то ИСПДн, обрабатывающие ПДн, должны следовать принципам проектирования систем безопасности информации. В данной базовой архитектуре определены некоторые компоненты обеспечения безопасности информации, которые имеют решающее значение для защиты ПДн. Представленная базовая архитектура основана на модели, приведенной в ГОСТ Р 57100.

Значимые вопросы, касающиеся базовой архитектуры защиты ПДн, приведены в разделе 6 и включают в себя принципы обеспечения безопасности ПДн, характерные для ИСПДн.

Базовая архитектура может быть представлена следующим образом:

- уровни технической базовой архитектуры, приведенные в 7.2, определяют ее с точки зрения компонентов. В каждом уровне сгруппированы компоненты, имеющие общую цель или сходную функцию;

- модель реализации, приведенная в 7.3, определяет базовую архитектуру с точки зрения автономной ИСПДн. Каждое представление показывает группировку компонентов в зависимости от их реализации в ИСПДн;

- представления, приведенные в 7.4, определяют базовую архитектуру с точки зрения взаимодействия. Эти представления демонстрируют взаимодействие компонентов между системами сторон, участвующих в обмене информацией.

Базовая архитектура предоставляет правила соответствия между значимыми вопросами и точками зрения посредством использования таблиц соответствия.

Центральным элементом базовой архитектуры является создаваемая ИСПДн. Субъект ПДн использует ИСПДн. На проектирование ИСПДн оказывают влияние значимые вопросы, рассматриваемые в настоящем стандарте, а также другие значимые вопросы. К другим значимым вопросам можно отнести вопросы, которые касаются нефункциональных требований, оказывающих влияние на качество функционирования, доступность и проектирование ИСПДн и не влияющих на функциональную обработку ПДн. Эти вопросы выходят за рамки применения настоящего стандарта.

ИСПДн может содержать компоненты из базовой архитектуры защиты ПДн, приведенной в настоящем стандарте, а также другие компоненты. Эти компоненты не обрабатывают ПДн, а имеют дело с другими функциональными возможностями ИСПДн, такими, как обеспечение доступности или предоставление специальных пользовательских интерфейсов. Такие компоненты также выходят за рамки применения настоящего стандарта.

4.2 Взаимосвязь с системой управления

Использование системы управления дает возможность операторам и обработчикам ПДн более эффективно выполнять требования защиты с помощью структурированного подхода. Структурированный подход предоставляет операторам ПДн возможность оценивать результаты и постоянно повышать эффективность системы управления.

Эффективная система управления является прозрачной в максимально возможной степени, но все же оказывает влияние на людей, процессы и технологии. Она должна быть частью программы внутреннего контроля и стратегии снижения рисков в организации, а ее реализация должна способствовать обеспечению соблюдения требований, установленных в [1].

5 Участники обработки персональных данных

5.1 Общие положения

Сторонами, участвующими в обработке ПДн, являются:

- субъект персональных данных;
- оператор персональных данных;
- обработчик ПДн, которому оператор персональных данных поручает обработку ПДн.

С точки зрения реализации базовая архитектура защиты ПДн разделена на три части. Каждая часть относится к реализованной ИСПДн с точки зрения каждого из участников.

ИСПДн, действующие субъекты и потоки ПДн между этими системами приведены на рисунке 1. Рисунок иллюстрирует логическое разделение функциональных возможностей базовой архитектуры защиты ПДн, описанной в настоящем стандарте. Он не предназначен для представления физической структуры, организации или аппаратных средств систем персональных данных.

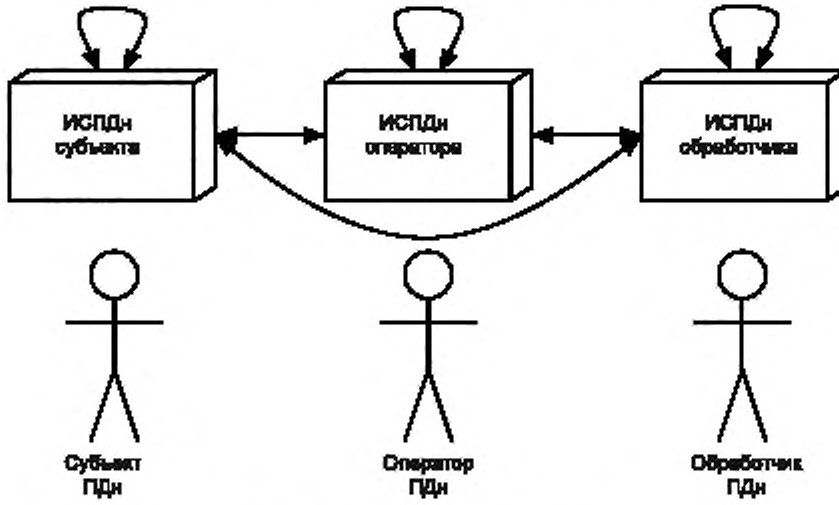


Рисунок 1 — Действующие субъекты и их информационные системы персональных данных в соответствии с настоящим стандартом

Действующий субъект может нести или не нести ответственность за создание используемых им ИСПДн. Например, субъект ПДн может использовать систему, созданную и являющуюся ответственностью оператора ПДн, или система субъекта ПДн может быть частью системы оператора ПДн. Кроме

того, функциональные возможности системы ПДн субъекта ПДн могут быть распределены по различным системам ПДн, владельцами которых являются субъект ПДн и оператор ПДн. Аналогичным образом оператор ПДн может предоставлять систему обработчику ПДн. Процессы обработки ПДн, в которых применяются ИСПДн, используют широкий спектр методов обмена информацией и моделей доверия. Базовая архитектура, приведенная в настоящем стандарте, основана на обобщении этих моделей.

Если оператор ПДн использует ИСПДн, находящуюся в организации, другие стороны, заинтересованные в обеспечении безопасности ПДн, могут налагать требования на эту систему. Например, система субъекта ПДн должна отвечать минимальным требованиям безопасности, чтобы иметь возможность подключаться к другим системам ПДн. Другие примеры включают в себя использование специальных компонентов обеспечения безопасности, таких как аппаратные устройства аутентификации, определенные версии операционной системы или специальные версии веб-браузера.

Примечания

1 В ИСПДн, например, использующих одноранговые коммуникации (способ связи, модель связи или технология связи, обеспечивающие коммуникации между являющимися равноправными объектами без центральных серверов), каждое приложение может брать на себя роли всех трех перечисленных действующих субъектов. Информация отправляется и принимается каждым равноправным узлом, поэтому каждый равноправный узел может быть оператором ПДн или обработчиком ПДн, которому другая сторона передала роль оператора персональных данных.

2 В приложениях социальных сетей ПДн могут обрабатываться любым пользователем, имеющим доступ к профилям других пользователей. Веб-приложения социальных сетей позволяют всем авторизованным и, возможно, анонимным пользователям сервиса обрабатывать ПДн (являться обработчиком), которые предоставлены подключенными к социальной сети субъектами ПДн.

5.2 Этапы жизненного цикла персональных данных при обработке

5.2.1 Сбор

Многие организации осуществляют сбор информации у субъектов ПДн. Осуществляя сбор персональных данных, организации должны учитывать предпочтительные способы защиты и законные права субъектов ПДн, а также требования обеспечения безопасности ПДн, установленные в [1]. На всех этапах обработки необходимо учитывать такие факторы, как тип ПДн, наличие согласия на обработку и необходимые способы защиты ПДн. Сбор ПДн следует осуществлять только в том случае, если он необходим для достижения заявленных целей.

С ПДн должна быть связана соответствующая документация. Примеры документации включают в себя (но не ограничиваются этим):

- программные теги, формулирующие цель(и), для которой(ых) могут использоваться ПДн;
- записи, описывающие цель(и), для которой(ых) могут использоваться ПДн;
- записи о данном субъектами ПДн согласии на обработку и о любых конкретных свойствах, которые необходимо отслеживать (например, специальные категории ПДн следует шифровать или удалять по истечении определенного периода времени).

Процессы сбора ПДн должны быть спроектированы таким образом, чтобы осуществлялся сбор только тех ПДн, которые необходимы для соответствующей транзакции. Организациям следует принимать меры для сведения к минимуму случайного/непреднамеренного сбора ПДн через системы ввода данных (например, формы веб-приложений, позволяющие вводить любую информацию). Ввод произвольных ПДн должен быть сведен к минимуму посредством использования полей ввода, учитывающих конкретные условия отображения, уменьшающего или устраняющего области в веб-форме, куда можно вводить такую информацию (например, удаляя ненужные кнопки-флажки и поля для свободного текста). Кроме того, следует рассмотреть вопрос использования полей с заранее определенными элементами (например, окна списка и «выпадающие» списки), содержащими не относящиеся к ПДн опции. Если необходимы текстовые поля произвольной формы, пользовательский интерфейс должен обеспечивать:

- предупреждения, предостерегающие субъекта ПДн, что он не должен вводить ПДн, кроме тех, что явно запрашиваются и на которые дается согласие на обработку, или тех, что требуются в соответствии с применимым законодательством;
- однозначное указание тех полей, куда должны вводиться ПДн, и того, какие ПДн должны быть введены (например, фамилия, адрес, информация о здоровье);
- однозначное указание тех полей, куда не следует вводить ПДн.

5.2.2 Передача

Передача, распространение или раскрытие ПДн другим лицам означают, что ПДн больше не находятся под единоличным контролем оператора ПДн. Термин «передача» обычно представляет собой термин, используемый для описания распространения ПДн от оператора или обработчика ПДн другим операторам и обработчикам ПДн. Если ПДн передаются от оператора ПДн другому действующему субъекту, передача может называться «раскрытием».

Ответственность и подотчетность за переданные ПДн следует согласовывать и поддерживать каждой стороной, участвующей в обработке ПДн. Такое соглашение должно быть составлено в письменной форме. Кроме того, такие соглашения должны соответствовать положениям [1] в исходном и целевом домене передачи. В соответствующих случаях или когда это требует законодательство, субъект ПДн должен быть уведомлен об осуществлении передачи и проинформирован о содержании и цели передачи. В случае возникновения спора между субъектом ПДн и оператором или обработчиком ПДн должны быть доступны записи соответствующих транзакций передачи ПДн для последующего применения письменных доказательств в разрешении любого подобного спора.

Передачи специальных категорий ПДн следует избегать, если только это:

- не является необходимым для предоставления услуги, которую запрашивает субъект ПДн с его письменного согласия на обработку ПДн;
- не отвечает требованиям для предложения запрашиваемой услуги;
- не регулируется положениями, указанными в [1].

Во время передачи ПДн следует применять соответствующие меры обеспечения безопасности ПДн. В случае передачи ПДн должны передаваться по защищенному каналу или в зашифрованном виде, если передача осуществляется по незащищенному каналу. Если ПДн передаются на физическом носителе информации, они должны быть зашифрованы. Если используется шифрование, ключ шифрования не должен храниться или передаваться вместе с зашифрованными ПДн.

5.2.3 Использование

Использование ПДн означает любую форму обработки ПДн, которая не включает «сбор», «передачу», «хранение», «архивирование» или «уничтожение». Принципы обеспечения безопасности ПДн, а также нормативные правовые акты, например [1], могут ограничивать обработку ПДн, если эта обработка несовместима с первоначально указанными целями. Соответственно ПДн должны обрабатываться только для заявленных целей, для которых осуществлялся их сбор.

Если ПДн требуется обрабатывать для другой цели, не охватываемой действующим законодательством, от субъекта ПДн или его представителя следует получить согласие на обработку. Субъекту ПДн должен быть предоставлен способ связи с оператором ПДн в случае возникновения любых вопросов о каких-либо действиях, которые не ясны субъекту ПДн.

В случаях, когда такая обработка считается необходимой, должно быть получено согласие субъекта ПДн, если иное не разрешено законом. Субъектам ПДн следует представлять четкое уведомление о конкретном использовании ПДн. Кроме того, должны быть применены механизмы защиты, соответствующие использованию ПДн. Механизмы защиты включают в себя использование методов обезличивания перед обработкой, а также применение методов безопасных вычислений во время обработки.

5.2.4 Хранение

Одним из условий хранения ПДн является наличие согласия субъекта ПДн на применение конкретных мер в соответствии с действующим законодательством. В таких случаях ПДн должны храниться только в течение времени, необходимого для достижения конкретной бизнес-цели.

ПДн должны храниться с применением соответствующих мер защиты и механизмов для предотвращения несанкционированного доступа, модификации, уничтожения, удаления или иного несанкционированного использования. Такие меры защиты включают в себя (но не ограничиваются) шифрование и обезличивание.

Архивирование ПДн требует особого внимания. Принципы обеспечения безопасности ПДн определяют, что ПДн следует сохранять только до тех пор, пока это необходимо для выполнения заявленных целей, а затем их следует безопасно уничтожить или обезличить. Однако, если оператору ПДн или обработчику ПДн в соответствии с действующим законодательством требуется сохранение ПДн после истечения срока действия других целей, ПДн должны быть заблокированы (т. е. архивированы и защищены с помощью механизма управления доступом для предотвращения дальнейшего использования). Основные соображения при архивировании ПДн должны заключаться в обеспечении уверенности в наличии соответствующих механизмов защиты ПДн, включая решения по управлению доступом, обеспечивающие доступ к архивированной ПДн только уполномоченным пользователям.

Оператор ПДн должен реализовать меры защиты для уничтожения ПДн в системах хранения по истечении срока действия цели хранения или в случае, когда цель хранения или обработки ПДн больше не являются действительными.

5.2.5 Уничтожение

На завершающем этапе жизненного цикла ПДн происходит удаление или уничтожение ПДн. Конкретные ПДн в записях могут быть заблокированы от несанкционированного использования путем их маркировки для уничтожения. Следует отметить, что удаление ПДн не обязательно означает, что ПДн уничтожаются окончательно, так как удаленные ПДн в информационных системах могут быть восстановлены. Хотя эта задача может казаться очевидной при обработке ПДн, процедуры, касающиеся уничтожения ПДн, иногда не соответствуют требованиям защиты. Перед уничтожением ПДн должны учитываться спецификации, представленные оператором ПДн (например, цель использования), или требования, установленные законодательством (например, дата истечения срока действия для конкретных ПДн).

6 Значимые вопросы

6.1 Общие положения

Значимыми, как определено в ГОСТ Р 57100, считаются вопросы, отражающие необходимость обеспечения безопасности ПДн для одной или нескольких сторон взаимодействия. Базовая архитектура защиты ПДн, приведенная в настоящем стандарте, отражает наиболее значимые вопросы защиты для сторон, связанных с обработкой ПДн. Значимые вопросы касаются принципов обеспечения безопасности ПДн и требований защиты ПДн, вытекающих из этих принципов и согласующихся с ними.

Все установленные требования обеспечения безопасности ПДн должны соответствовать действующему законодательству и/или определяться в соответствии с процессом управления рисками нарушения безопасности ПДн. Организации, проектирующие систему, которая обрабатывает ПДн, должны следовать этому процессу перед составлением модели угроз и модели нарушителя.

6.2 Принципы обеспечения безопасности персональных данных

Оператор ПДн отвечает за обеспечение защиты ПДн и за легитимное обращение с ней в любое время в масштабах всей организации, а также за обработку ПДн, осуществляемую по поручению обработчиком ПДн.

Оператор ПДн несет полную ответственность за реализацию мер защиты при обработке ПДн. Меры защиты обеспечивают уверенность в том, что требования защиты, установленные для конкретного субъекта ПДн, транзакции или сценария, учитываются и последовательно выполняются. Подтверждение реализации мер защиты следует обеспечивать путем надлежащего документального оформления существующих мер защиты и предоставления заключения стороны, подтверждающей наличие таких мер, их правильную реализацию и надлежащее функционирование. В конечном счете оператор ПДн должен признавать и соблюдать принципы обеспечения безопасности ПДн, такие как:

- согласие и выбор;
- законность цели и ее спецификация;
- ограничение на сбор информации;
- минимизация данных;
- ограничения в отношении использования, хранения и раскрытия;
- точность и качество ПДн;
- открытость, прозрачность и уведомление;
- персонифицированный доступ;
- ответственность;
- обеспечение безопасности информации;
- соответствие требованиям нормативной правовой базы.

6.3 Требования защиты персональных данных

Информационные системы персональных данных должны реализовывать меры защиты как основной элемент на каждом этапе жизненного цикла ПДн. Требования защиты дают возможность разработчику системы реализовать связь между принципами обеспечения безопасности ПДн и компонентами архитектуры, приведенными в разделе 7.

Для реализации эффективных мер защиты в ИСПДн следует разработать схемы потоков, описывающих обработку ПДн. Блок-схемы обработки ПДн являются графическим представлением потока ПДн через ИСПДн и между различными участниками обмена ПДн. Например, если оператор передает ПДн обработчику, блок-схема обработки ПДн должна содержать элемент передачи ПДн.

Блок-схема обработки ПДн может быть представлена в виде таблицы потоков ПДн. В указанной таблице отслеживаются процессы сбора, передачи, использования, хранения или уничтожения ПДн и может указываться такая информация, как тип ПДн, действующий субъект, осуществлявший сбор ПДн, цель обработки, действующий субъект, которому будут переданы ПДн, необходимость получения согласия от субъекта ПДн, период хранения и место, где будут храниться ПДн, а также результирующий уровень риска нарушения безопасности ПДн. Таблица потоков ПДн используется в процессе управления рисками нарушения безопасности ПДн, на ее основе формируются модель угроз и модель нарушителя безопасности ПДн.

После завершения анализа требований разработчикам ИСПДн следует использовать перекрестные ссылки между требованиями защиты ПДН в ИСПДн и перечнем значимых вопросов, рассмотренных в настоящем стандарте. Затем требования защиты следует использовать для выбора компонентов архитектуры защиты ПДн, удовлетворяющих указанным требованиям.

В приложении А содержится примерный перечень значимых вопросов и описание взаимосвязи значимых вопросов с принципами обеспечения безопасности ПДн и компонентами базовой архитектуры защиты ПДн, приведенными в настоящем стандарте.

7 Архитектурные представления

7.1 Общие положения

Архитектурные представления в данном разделе систематизированы по трем видам (уровням):

- представление с точки зрения компонентов;
- представление с точки зрения субъектов (сторон);
- представление с точки зрения взаимодействия.

Представление с точки зрения компонентов описывает компоненты ИСПДн и разделяет их по уровням на основе их функциональных возможностей. Каждый уровень группирует компоненты, вносящие свой вклад в надлежащую обработку ПДн. Для каждого компонента приводится краткое руководство по реализации. Там, где это применимо, приводится руководство для оператора или обработчика ПДн. Это представление полезно для понимания компоновочных блоков в базовой архитектуре защиты ПДн. В представлении с точки зрения компонентов содержатся таблицы, показывающие примеры типичных взаимосвязей между принципами обеспечения безопасности ПДн и компонентами архитектуры защиты ПДн. Такие таблицы соответствия полезны для понимания того, как в ИСПДн соблюдаются принципы обеспечения безопасности ПДн. Аналогичные таблицы могут использоваться в качестве примеров и обновляться в ходе разработки системы с целью описания соблюдения принципов обеспечения безопасности ПДн в конкретной ИСПДн.

Представление субъекта рассматривает компоненты, описанные в представлении компонента, с точки зрения ИСПДн отдельного субъекта ПДн. Эта точка зрения полезна при проектировании архитектуры защиты ПДн для конкретной ИСПДн.

Представление взаимодействия рассматривает компоненты с точки зрения развертывания. Эта точка зрения полезна для понимания того, как компоненты в ИСПДн различных субъектов взаимодействуют друг с другом.

7.2 Представление с точки зрения компонентов

7.2.1 Общие положения

Представление с точки зрения компонентов предназначено для описания компонентов ИСПДн, которые участвуют в обработке ПДн.

При выборе компонентов следует руководствоваться соответствующими требованиями защиты ПДн. Разработчик ИСПДн для конкретного(ых) действующего(их) субъекта(ов) должен использовать данное представление для определения компонентов, которые необходимо включить в архитектуру разрабатываемой им системы. Эта архитектура должна основываться на требованиях обеспечения безопасности ПДн, установленных с использованием указаний, приведенных в разделе 7. Следует отметить, что не все компоненты, описанные в настоящем стандарте, обязательно подходят для конкретной ИСПДн.

Представление с точки зрения компонентов сгруппировано по трем уровням. Каждый уровень представляет собой логическую группу компонентов, которые способствуют достижению определенной цели при обработке ПДн. Компоненты на уровне установок по обеспечению безопасности ПДн относятся к управлению метаданными, связанными с обработкой ПДн, включая обмен информацией о целях обработки, согласии и предпочтительных способах обеспечения безопасности ПДн конкретного субъекта ПДн. Компоненты на уровне управления идентификационными данными и управления доступом отвечают за обеспечение уверенности в использовании правильной идентификационной информации при обработке ПДн и осуществлении управления доступом к ПДн в соответствии с требованиями обеспечения безопасности ПДн. Наконец, компоненты на уровне ПДн выполняют различные задачи по обработке ПДн.

Базовая архитектура защиты ПДн разработана с использованием предположения, что все компоненты взаимодействуют с несколькими другими компонентами. Однако для поддержания универсальности и удобочитаемости возможные взаимодействия между компонентами в представлении были опущены.

Некоторыми из компонентов базовой архитектуры являются технологии, улучшающие (обеспечивающие) конфиденциальность ПДн. Данный выбор технологий не является исчерпывающим. Существуют другие технологии, улучшающие (обеспечивающие) конфиденциальность ПДн, которые не описаны в настоящем стандарте. Разработчик ИСПДн отвечает за выбор соответствующих технологий и за их применение в данной базовой архитектуре.

Пример архитектуры ИСПДн, которая применяет технологии, улучшающие (обеспечивающие) конфиденциальность при обработке ПДн, приведен в приложении Б.

Пример использования мандатов на основе атрибутов для создания ИСПДн [2], обеспечивающей управление обезличенными идентификационными данными и управление доступом, приведен в приложении В.

В следующих пунктах настоящего стандарта описываются уровни архитектуры, входящие в них компоненты и действующие субъекты, взаимодействующие с компонентами. Кроме того, приводится общее описание каждого компонента и следуют указания, касающиеся конкретных действующих субъектов. Для некоторых компонентов не приводится никаких указаний, характерных для ИСПДн конкретного действующего субъекта, поскольку поведение этого компонента в разных ИСПДн имеет схожий характер.

7.2.2 Уровень установок политики защиты

7.2.2.1 Общие положения

Уровень установок политики защиты составляют компоненты, сообщающие политику защиты ИСПДн операторов и реализующие требования обеспечения безопасности ПДн. Эти компоненты позволяют разрабатывать политику и реализовывать соответствующие меры защиты в ИСПДн.

Кроме того, компоненты на этом уровне должны передавать оператору ПДн и обработчику ПДн информацию о предпочтительных способах защиты ПДн и согласии на обработку, которую подписал субъект ПДн.

7.2.2.2 Доведение политики и целей

Общее описание

Данный компонент отвечает за передачу информации, включая обновления, информацию о политике защиты ПДн оператора ПДн и целях сбора ПДн в ИСПДн.

Переданная информация должна содержать, по крайней мере, следующее:

- идентификационные данные операторов ПДн и любых взаимосвязанных обработчиков ПДн;
- политики, касающиеся передачи ПДн обработчикам ПДн;
- применяемые технологии, улучшающие (обеспечивающие) конфиденциальность ПДн (например, обезличивание), с их соответствующими задачами,
- цели, для которых осуществляется сбор ПДн;
- идентификацию ПДн, которые должны быть собраны;
- юридические права субъекта ПДн на получение доступа к своим ПДн для определения объема хранящихся его ПДн, а также проверки и исправления любых неточностей, и процедуры осуществления этого.

Субъект ПДн

Субъект ПДн, получивший извещение о политике и целях компонента ИСПДн от оператора ПДн, должен:

- получать информацию о политике и целях от соответствующего компонента ИСПДн оператора ПДн;
- интерпретировать полученную информацию с целью ее отображения субъекту ПДн понятным образом;
- получать предложение возможности локального хранения полученной информации;
- подтверждать оператору ПДн факт получения информации о политике и целях субъектом ПДн.

Оператор ПДн

Оператор ПДн, как связанный с публикацией политики и целей компонента ИСПДн, находящейся под контролем оператора ПДн, должен:

- хранить информацию о политике и целях, которая была передана субъектам ПДн;
- регистрировать действия по передаче информации о политике и целях субъектам ПДн таким образом, чтобы можно было установить, в какое время и какая информация была актуальна и передавалась субъектам ПДн, наряду с подтверждением получения этой информации;
- передавать текущую информацию о политике и целях соответствующему компоненту ИСПДн субъекта ПДн таким образом, чтобы она могла быть использована этой системой для полного и понятного информирования субъекта ПДн или могла быть преобразована указанным компонентом в требуемую форму с помощью некоторого заранее определенного преобразования;
- передавать ссылку на отображаемую информацию о политике и целях тем компонентам, которые управляют хранением информации о согласии и хранением самих ПДн;
- передавать обновленные сведения об изменениях информации о политике и целях соответствующим компонентам, принадлежащим тем субъектам ПДн, которые дали согласие на получение такой информации.

Обработчик ПДн

ИСПДн обработчика ПДн должна получать копии политики защиты персональных данных и целей обработки от ИСПДн оператора ПДн. ИСПДн обработчика ПДн должна представлять документацию о политике защиты персональных данных и целях обработки, полученную от оператора ПДн, в ясной и понятной форме всем, кто имеет доступ к ПДн, регулируемой этой политикой. Оператор ПДн может условиться об обработке ПДн различными обработчиками ПДн. Связанный с публикацией целей компонент ИСПДн оператора ПДн должен передавать цели, относящиеся к предоставленным ПДн, всем соответствующим обработчикам ПДн. Каждый обработчик ПДн должен быть проинформирован о цели(ях) обработки ПДн.

7.2.2.3 Классификация персональных данных

Общее описание

Система, обрабатывающая ПДн, должна быть осведомлена о классах (категориях) ПДн, которые она обрабатывает, с тем чтобы можно было проводить различие между разными типами данных (например, специальные категории ПДн, ПДн и информация, не являющаяся ПДн). Это необходимо для обработки ПДн разными способами в зависимости от категории ПДн. Кроме того, ИСПДн должна быть осведомлена о значениях ПДн, которые содержат прямые идентификаторы, такие, например, как имя или индивидуальный номер налогоплательщика. Этот компонент должен выполнять функции, обеспечивающие такую классификацию в ИСПДн.

При работе с информацией, не являющейся ПДн, следует понимать и оценивать риск объединения информации, не являющейся ПДн, для выведения или получения идентификационных данных или профиля уникального пользователя или, по крайней мере, достаточно небольшого подмножества пользователей.

Все ПДн должны быть надлежащим образом классифицированы, чтобы они могли обрабатываться и храниться в ИСПДн в соответствии с их промаркированной категорией. Если ПДн были собраны случайно, например в результате незапрошенного ввода, осуществление этого может оказаться невозможным, и, соответственно, должны приниматься меры для сведения к минимуму возможности сбора незапрошенных ПДн. Хотя ИСПДн должна быть осведомлена о значениях ПДн, содержащих прямые идентификаторы, выполнение этого может быть невозможным в случае сбора незапрошенных ПДн.

Субъект ПДн

ИСПДн субъекта ПДн должна быть способна идентифицировать классификационную маркировку, связанную с ПДн, и должна обрабатывать ПДн в соответствии с их классификацией. Классификация может также использоваться для идентификации ПДн, которым следует обеспечивать защиту с использованием технологий, улучшающих (обеспечивающих) конфиденциальность персональных данных.

Компонент классификации ПДн также обеспечивает дальнейшую классификацию ПДн по подкатегориям, где подкатегории являются требованием конкретной сферы применения.

Оператор ПДн

ИСПДн оператора должна содержать полную классификацию ПДн, используемую в системах, обрабатывающих классифицированные ПДн. Эта информация должна передаваться обработчикам ПДн. Кроме того, классификация ПДн может использоваться для компонентов протоколирования, обезличивания, раскрытия, архивирования и хранения ПДн, чтобы они могли определять, какие части данных содержат ПДн.

Обработчик ПДн

ИСПДн обработчика должна быть способна обрабатывать классифицированные ПДн. Эта информация должна использоваться для аудита ПДн и обеспечения безопасности ПДн.

7.2.2.4 Управление согласиями на обработку персональных данных

Общее описание

Согласие субъекта ПДн является необходимым условием обработки ПДн, если такая обработка иначе не разрешена законодательством.

Этот компонент связан с задачами управления согласиями и включает в себя (но не ограничиваясь) следующее:

- получение осознанного согласия субъекта ПДн;
- хранение информации о согласии в ИСПДн заинтересованной стороны;
- связывание хранящейся информации о согласии с версией информации о политике и целях, для которых было дано согласие;
- проверку наличия согласия перед обработкой ПДн;
- поддержку статуса информации о согласии.

Нормативные правовые акты могут иметь преимущество в случае отсутствия или ограничения согласия, выраженного субъектом ПДн.

Субъект ПДн

Оператор ПДн должен получать осознанное согласие субъекта ПДн с помощью компонента управления согласиями в ИСПДн субъекта ПДн. При определенных обстоятельствах субъект ПДн может изменить или отозвать согласие, и эта информация должна быть передана ИСПДн оператора.

Оператор ПДн

В ИСПДн оператора этот компонент должен поддерживать актуальную информацию о статусе согласия. ИСПДн оператора должна быть способна находить, хранить, управлять и поддерживать информацию о согласии.

ИСПДн оператора должна передавать информацию о согласии другим сторонам, которым она требуется. Кроме того, этот компонент должен принимать обновления статуса согласия субъекта ПДн (например, изменение или отзыв согласия). ИСПДн оператора должна представлять и распространять эту информацию по мере необходимости.

Обработчик ПДн

ИСПДн обработчика должна проверять наличие согласия всех субъектов ПДн, связанных с предоставляемыми ей ПДн. Эта информация должна поступать от ИСПДн оператора. Перед любой обработкой ИСПДн обработчика следует удостовериться, что ИСПДн содержит актуальную информацию о согласии соответствующих субъектов ПДн. ИСПДн обработчика должна быть готова принимать изменения статуса согласия, когда о таких изменениях уведомляет оператор ПДн.

7.2.2.5 Управление способами защиты персональных данных

Общее описание

В некоторых ситуациях возможно, что субъект ПДн может выразить свои предпочтения относительно того, как будут обрабатываться его ПДн оператором или обработчиком ПДн. В этих случаях соответствующие ИСПДн действующих субъектов должны быть способны зафиксировать эти предпочтительные способы обработки и сообщить о них оператору или обработчику ПДн. Оператор и обработчик ПДн должны быть способны понимать эти предпочтительные способы обработки и в максимально возможной степени соблюдать их при обработке ПДн.

Субъект ПДн

Если обработка ПДн основана на установках предпочтительных способов обеспечения безопасности ПДн, то субъекту ПДн должен предоставляться интерфейс для выбора установок, наиболее подходящих для этих целей. Например, сюда могут входить установки, определяющие, как ИСПДн использует, передает или раскрывает ПДн.

Оператор ПДн

Если субъект ПДн определил какие-либо предпочтительные способы обеспечения безопасности ПДн, то оператор ПДн должен представить эти варианты субъекту ПДн.

Оператор ПДн должен реализовывать соответствующие предпочтительные способы обеспечения безопасности ПДн, которые указал субъект ПДн из имеющихся вариантов, если таковые существуют. Оператор также должен распространять эту информацию любым сторонам, которые обрабатывают ПДн, связанную с этими способами.

Обработчик ПДн

Если это имеет отношение к установленным задачам обработчика ПДн, ИСПДн обработчика должна быть осведомлена о любых ограничениях, устанавливаемых для обработки ПДн выбранными предпочтительными способами обеспечения безопасности ПДн, которые указал субъект ПДн, и действовать в соответствии с ними. Эта информация и ее возможные обновления должны быть получены от оператора ПДн или непосредственно от субъекта ПДн через их соответственные ИСПДн.

7.2.2.6 Взаимосвязь между принципами обеспечения безопасности персональных данных и компонентами на уровне установок

Пример взаимосвязи между принципами обеспечения безопасности ПДн и компонентами на уровне установок приведен в таблице 1. Обозначение «X» в таблице указывает на взаимосвязь между компонентом данного уровня и принципом, однако указанная взаимосвязь приводится только в качестве примера.

Таблица 1 — Пример взаимосвязи между принципами обеспечения безопасности персональных данных и компонентами на уровне установок

Компоненты	Принципы										
	Согласие и выбор	Законность цели и ее спецификация	Ограничение на сбор информации	Минимизация данных	Ограничения в отношении использования, хранения и раскрытия	Точность и качество	Открытость, прозрачность и уведомление	Индивидуальное участие и доступ	Ответственность	Обеспечение безопасности информации	Соответствие
Доведение политики и целей	X	X	X	X	—	—	X	—	X	—	X
Классификация ПДн	—	—	X	X	X	—	—	—	—	—	—
Управление согласиями	X	X	X	—	—	—	—	X	—	—	—
Управление предпочтительными способами защиты персональных данных	X	X	X	—	X	—	X	—	—	—	—

7.2.3 Уровень управления идентификационными данными и управления доступом

7.2.3.1 Общие положения

Компоненты на уровне управления идентификационными данными и управления доступом помогают идентифицировать действующих субъектов и их ИСПДн и управлять соответствующей идентификационной информацией. Кроме того, компоненты на этом уровне управляют доступом к ПДн действующих субъектов. Компоненты реализуют следующие функциональные возможности:

- управление идентификационными данными сторон, заинтересованных в обеспечении безопасности ПДн;
- управление идентификационными данными действующих субъектов, использующих ИСПДн;
- предоставление этой информации другим компонентам в ИСПДн;
- управление соответствием между идентификационными данными субъекта ПДн и обезличенными ПДн.

Уровень управления идентификационными данными и управления доступом предоставляет идентификационную информацию компонентам на других уровнях, которым это требуется. Следует отме-

тить, что в настоящем стандарте не специфицируются методы управления идентификационными данными, которые должны использоваться.

7.2.3.2 Управление идентификационными данными

Общее описание

Данный компонент может иметь несколько назначений, каждое из которых может быть реализовано отдельной системой управления идентификационными данными.

Во-первых, данный компонент может осуществлять управления идентификационными данными субъектов ПДн, персональные данные которых обрабатываются в системе. Во-вторых, этот компонент может управлять идентификационными данными пользователей ИСПДн, которые обрабатывают ПДн субъектов. В-третьих, данный компонент может осуществлять управление идентификационными данными ИСПДн, заинтересованных в защите персональных данных. Это дает возможность ИСПДн различных сторон взаимно аутентифицировать друг друга во время передачи ПДн. Данный перечень примеров назначений данного компонента не является исчерпывающим.

Механизмы определения характера и точности базовой идентификационной информации не приводятся в настоящем стандарте. Функциональные возможности компонента управления идентификационными данными одинаковы для всех действующих сторон.

7.2.3.3 Обезличивание

Общее описание

Если при обработке ПДн используется обезличивание, то задействованные ИСПДн должны иметь функции управления используемыми методами обезличивания.

Примечание — Для обезличивания применяются различные методы, например метод введения идентификаторов, метод изменения состава или семантики, метод декомпозиции, метод перемешивания и, кроме того, может применяться шифрование ПДн.

Компонент системы обезличивания на уровне управления идентификационными данными и управления доступом содержит информацию о реализованной системе обезличивания и ее параметрах. Например, если используется шифрование, этот компонент хранит информацию об используемых ключах.

Взаимосвязанный компонент обезличивания ПДн на уровне ПДн используется для их фактического преобразования.

Субъект ПДн

Если в ИСПДн субъекта используется обезличивание, то система должна содержать описание реализованного метода обезличивания. Компонент обезличивания на уровне ПДн системы персональных данных субъекта ПДн должен применять данный метод обезличивания.

Оператор ПДн

Управление методами обезличивания может осуществляться ИСПДн оператора. В этом случае ИСПДн оператора передает информацию о методах обезличивания, используемых в ИСПДн субъекта и обработчиков ПДн. Эта информация может потребоваться для обеспечения уверенности в том, что подвергшиеся обезличиванию ПДн из системы субъекта ПДн могли быть обработаны в ИСПДн оператора и ИСПДн обработчика. Следует отметить, что может потребоваться определение нескольких вариантов (реализованных методов) обезличивания, например для осуществления обезличивания ПДн разными методами для различных обработчиков.

Обработчик ПДн

Если обработчику ПДн нужно выполнять обезличивание в соответствии с инструкциями оператора ПДн, ему следует реализовать данный компонент для осуществления управления реализованными методами обезличивания.

7.2.3.4 Управление доступом

Общее описание

Механизмы управления доступом должны обеспечивать уверенность в том, что доступ к функциям в ИСПДн предоставляется только в рамках ограничений, установленных на основе требований защиты. Например, если сбор у субъектов ПДн осуществляется с использованием веб-формы и осуществляется в течение определенного периода времени, доступ к веб-форме должен предоставляться только в течение данного времени. В этом примере ИСПДн оператора должна ограничивать доступ субъектов ПДн к форме сбора ПДн.

Функциональные возможности компонента управления доступом одинаковы для всех действующих субъектов. Правила и методы управления доступом в каждой ИСПДн выводятся из требований обеспечения безопасности ПДн.

7.2.3.5 Аутентификация

Общее описание

Аутентификация является важным компонентом обеспечения безопасности системы, обрабатывающей ПДн. Она обеспечивает уверенность в конфиденциальности и целостности ПДн, сбор, хранение и обработку которой осуществляет ИСПДн.

Компонент аутентификации может иметь несколько назначений. Во-первых, он может управлять аутентификацией пользователей, работающих с ИСПДн. Во-вторых, он может управлять взаимной аутентификацией ИСПДн или их компонентов в рамках безопасного доступа к ПДн и их передачи. Этот перечень примеров не является исчерпывающим.

Правила и методы, используемые при каждой реализации ИСПДн, следует рассматривать отдельно с учетом целей обеспечения безопасности действующего субъекта, который использует данную систему. Например, ИСПДн действующего субъекта должна аутентифицировать субъектов ПДн, использующих систему. Аналогичным образом ИСПДн субъекта должна аутентифицировать оператора ПДн перед передачей ПДн в ИСПДн этого оператора.

Функциональные возможности компонента аутентификации одинаковы в ИСПДн всех взаимодействующих сторон.

7.2.3.6 Авторизация

Общее описание

В ИСПДн, где ограничивается доступ любого действующего субъекта, должна существовать система авторизации. Доступ к ПДн должен предоставляться только авторизованным пользователям системы. Например, субъекты ПДн, выбранные для обработки ПДн, могут получать доступ к ПДн, к которым они имеют отношение.

Функциональные возможности компонента авторизации одинаковы для всех действующих субъектов. Правила и методы авторизации в каждой ИСПДн основываются на требованиях защиты ПДн.

7.2.3.7 Взаимосвязь между принципами обеспечения безопасности персональных данных и компонентами на уровне управления идентификационными данными и управления доступом

Пример установления соответствия между принципами обеспечения безопасности ПДн и компонентами на уровне управления идентификационными данными и управления доступом приведен в таблице 2. Обозначение «X» в таблице указывает на взаимосвязь между компонентом данного уровня и принципами обеспечения безопасности ПДн; однако указанная взаимосвязь приводится только в качестве примера.

Таблица 2 — Пример взаимосвязи между принципами обеспечения безопасности и компонентами на уровне управления идентификационными данными и управления доступом

Компоненты	Принципы										
	Согласие и выбор	Законность цели и ее спецификация	Ограничение на сбор информации	Минимизация данных	Ограничения в отношении использования, хранения и раскрытия	Точность и качество	Открытость, прозрачность и уведомление	Индивидуальное участие и доступ	Ответственность	Обеспечение безопасности информации	Соответствие
Управление идентификационными данными	—	—	—	—	X	—	X	—	—	X	—
Обезличивание	—	—	—	X	X	—	—	—	X	X	—
Управление доступом	—	—	—	—	X	X	—	X	X	X	—
Аутентификация	—	—	—	—	X	X	—	X	X	X	—
Авторизация	—	—	—	—	X	X	—	X	X	X	—

7.2.4 Уровень персональных данных

Компоненты на уровне ПДн должны реализовывать следующие функциональные возможности:

- сбор и передачу ПДн;
- обработку ПДн, включая безопасную обработку, и представление;
- хранение и архивирование ПДн;
- аудит ПДн и регистрацию происходящих с ними транзакций.

В настоящем стандарте определяются только общие требования управления ПДн, оставляя конкретные подробности на рассмотрение разработчика ИСПДн. Для снижения риска нарушения безопасности ПДн во время обработки должны использоваться соответствующие меры защиты.

Уровень ПДн использует информацию, поступающую с уровня установок, для введения в действие мер, основанных на требованиях обеспечение безопасности ПДн.

7.2.4.1 Управление персональными данными

Общее описание

Любая система, обрабатывающая ПДн, должна иметь определенные базовые функции для управления ПДн в системе. К ним относятся ввод, доступ, обновление и удаление ПДн. В случае необходимости ИСПДн должна быть способна поддерживать непрерывный процесс, обеспечивающий сбор и обработку ПДн в течение всего срока службы системы.

Субъект ПДн

Компонент управления персональными данными в ИСПДн субъекта связан со сбором и локальной обработкой ПДн, полученных у субъекта ПДн.

Оператор ПДн

Компонент управления персональными данными в ИСПДн оператора должен быть способен осуществлять обмен ПДн с ИСПДн субъектов (сбор ПДн) и обработчиков ПДн (для делегирования обработки). Следует отметить, что политика защиты персональных данных, а также использование различных технологий, улучшающих (обеспечивающих) конфиденциальность ПДн субъектов и другие факторы могут ограничивать инструментальные средства управления ПДн, доступные в ИСПДн оператора ПДн. Например, в системе оператора ПДн может быть запрещено добавлять ПДн или связывать ПДн с другой информацией.

Обработчик ПДн

Компонент управления ПДн ИСПДн обработчика ПДн обрабатывает ПДн, полученные от оператора ПДн.

7.2.4.2 Передача персональных данных

Общее описание

Компонент передачи ПДн отвечает за обмен ПДн между ИСПДн различных сторон, заинтересованных в защите ПДн. Передача ПДн должна включать взаимную аутентификацию и шифрование между исходной точкой и точкой назначения, чтобы защитить передачу ПДн и обеспечить их конфиденциальность. В этом случае компонент передачи ПДн должен использовать компоненты аутентификации и шифрования ПДн.

7.2.4.3 Проверка точности персональных данных

Общее описание

Должна осуществляться проверка корректности обрабатываемых ПДн на предмет точности данных и корректности формата. Оператор должен обладать достаточной информацией о данных и диапазоне их допустимых значений, чтобы предупреждать сторону, использующую систему, о возможных ошибках ввода ПДн.

Субъект ПДн

ИСПДн субъекта ПДн осуществляет проверку правильности данных, собранных у субъекта (субъектов) ПДн.

Оператор ПДн

Даже если ИСПДн субъекта спроектирована для осуществления проверки правильности ПДн, система оператора ПДн должна выполнять такую же проверку и, возможно, дополнительные проверки для обеспечения уверенности в точности данных и корректности формата ПДн. ИСПДн оператора может также осуществлять глобальные проверки на предмет посторонних значений и статистических отклонений.

Обработчик ПДн

ИСПДн обработчика должна выполнять обязанности, сходные с обязанностями системы оператора ПДн.

7.2.4.4 Обезличивание персональных данных

Общее описание

Компонент обезличивания на уровне ПДн использует систему обезличивания, описанную на уровне управления идентификационными данными и управления доступом, связанную с заменой идентификаторов, раскрывающих подлинные идентификационные данные субъекта ПДн, на обезличенные, скрывающие подлинные идентификационные данные.

Другой способ достижения целей обезличивания ПДн заключается с том, что информация делается частично анонимной.

Примеры возможного применения обезличивания ПДн включают в себя случаи, когда:

- идентификационные данные субъекта ПДн не требуются для достижения целей обработки ПДн;
- для обработки ПДн требуется идентификатор (например, при применении для обезличивания метода введения идентификатора).

Субъект ПДн

ИСПДн субъекта ПДн осуществляет обезличивание собранных ПДн перед их отправкой в ИСПДн оператора.

Оператор ПДн

Компонент обезличивания в ИСПДн оператора может использоваться для обработки подвергшихся обезличиванию идентификационных данных в ПДн, полученных от ИСПДн субъекта. Если система обезличивания основана на двусторонней функции, совместно используемой субъектом ПДн и оператором ПДн, последний может также повторно идентифицировать ПДн, когда это необходимо. ИСПДн оператора может также использовать обезличивание ПДн, которые передаются в систему обработчика ПДн. При раскрытии ПДн различным взаимодействующим сторонам (субъектам) следует использовать различные или по-разному параметризованные функции обезличивания.

Например, если ПДн передается в ИСПДн нескольких обработчиков ПДн, то для снижения риска сговора между обработчиками для ПДн, предоставляемых каждому обработчику, должны использоваться разные функции обезличивания. Оператор ПДн ведет реестр обработчиков ПДн и применяемых ими методов, а также параметров обезличивания. Кроме того, каждый случай раскрытия ПДн должен регистрироваться обеими сторонами, а транзакции раскрытия — системами оператора ПДн и обработчика ПДн.

Обработчик ПДн

ИСПДн обработчика может осуществлять обезличивание, если ей даются такие инструкции оператором ПДн.

7.2.4.5 Распределение секрета

Общее описание

Распределение секрета — это метод разделения значений ПДн на части, которые по отдельности не раскрывают никакую информацию об исходном значении. Распределение секрета может быть использовано для сбора ПДн с целью снижения риска нарушения безопасности ПДн. Распределение секрета обеспечивает более высокую защищенность ПДн в ИСПДн субъекта ПДн в сочетании с безопасными многосторонними вычислениями.

Распределение секрета может быть использовано для снижения риска со стороны нарушителей, так как сторона, имеющая доступ к части значений ПДн, не может узнать из них исходное значение. Это существенно усложняет атаки со стороны нарушителей. Для получения оптимальных результатов распределения секрета требуется наличие в системе более чем одного представителя каждого действующего субъекта. Каждый представитель должен хранить и обрабатывать ограниченное число частей ПДн.

Субъект ПДн

ИСПДн субъекта может осуществлять распределение секрета для ПДн, собранных у субъектов ПДн. Полученные части затем передаются операторам ПДн.

Оператор ПДн

ИСПДн оператора может использовать распределение секрета для обработки прошедших распределение секрета ПДн, полученных от системы субъекта ПДн, или для осуществления распределения секрета в отношении представленных открытым текстом ПДн до их передачи в систему обработчика ПДн.

Обработчик ПДн

ИСПДн обработчика может использовать распределение секрета для одной из целей. Во-первых, хранение или загрузка ПДн, прошедших распределение секрета, до их обработки. В этом случае ПДн

хранятся в форме с распределением секрета, но восстанавливаются перед обработкой. Во-вторых, использование в сочетании с безопасными многосторонними вычислениями. В этом случае можно выполнять вычисления непосредственно с ПДн, прошедшими распределение секрета.

7.2.4.6 Шифрование персональных данных

Общее описание

Компоненты шифрования ПДн могут обеспечивать применение механизмов шифрования ПДн перед их хранением. Проектирование ИСПДн может включать в себя определение того, какие хранящиеся ПДн должны быть зашифрованы. В зависимости от требований защиты обеспечения безопасности ПДн ключи шифрования могут совместно использоваться системами ИСПДн так, чтобы каждая из них могла расшифровывать ПДн и получать к ним соответствующий доступ. Если используется метод безопасных вычислений, способный обрабатывать зашифрованные ПДн, то для обработки не требуется выполнять процедуру расшифровывания информации.

Сервисы компонента могут включать в себя управление ключами, шифрованием ПДн в базах данных и шифрованием хранящихся ПДн, таких как резервные файлы и архивы. При этом проектирование и реализация методов шифрования ПДн должны проводиться в соответствии с действующими нормативными правовыми актами.

Шифрование ПДн может использоваться для защиты хранящихся ПДн. Это может осуществляться с двумя целями. Во-первых, можно хранить зашифрованные ПДн для предотвращения несанкционированного доступа к ним. Если они требуют обработки, осуществляется процедура расшифровывания с помощью соответствующего ключа. Шифрование ПДн снижает риск утечки данных из резервных копий. Во-вторых, ПДн могут быть зашифрованы для подготовки их к обработке в зашифрованном виде с использованием методов безопасных вычислений согласно действующим нормативным правовым актам.

7.2.4.7 Использование персональных данных

Общее описание

Для использования ПДн в вычислениях или анализе в ИСПДн действующего субъекта должен реализоваться компонент использования ПДн. В этом компоненте реализована логика обработки ПДн. Следует отметить, что для некоторых сценариев использования ПДн для снижения рисков потери ПДн могут применяться безопасные вычисления.

7.2.4.8 Безопасные вычисления

Безопасные вычисления могут использоваться для того, чтобы дать возможность операторам ПДн и обработчикам ПДн обрабатывать ПДн, не имея доступа к исходным входным значениям. Вместо этого методы безопасных вычислений осуществляют вычисления с использованием ПДн, которые были преобразованы с помощью технологий, улучшающих конфиденциальность персональных данных, таких как шифрование или распределение секрета.

Подмножество методов безопасных вычислений, известное как безопасные многосторонние вычисления, представляет собой метод, при котором стороны могут совместно вычислять некоторое значение на основе индивидуально хранимых частей информации, не раскрывая в процессе обработки данные части друг другу. Для обеспечения оптимальной защиты от нарушений при безопасных многосторонних вычислениях должны быть задействованы несколько операторов ПДн или обработчиков ПДн и их ИСПДн, каждая со своей соответствующей информацией.

Безопасные вычисления могут снижать риск утечки ПДн из системы персональных данных действующего субъекта, так как ПДн не предоставляются обрабатывающей стороне в открытой форме.

7.2.4.9 Управление запросами

Общее описание

Компонент управления запросами ИСПДн оператора и/или обработчика ПДн реализуется для фильтрации входящих запросов. Например, сервис может отказаться отвечать на статистический запрос, если для этого запроса недостаточно входных данных. Хотя отказ отвечать на запрос все же предоставляет некоторую информацию заинтересованной в обеспечении безопасности ПДн стороне, которая делает этот запрос, данный метод все же следует рассматривать как применимый в определенных сценариях.

Управление запросами — это специальный метод, используемый в приложениях «добычи данных», для сведения к минимуму обработки ПДн. Этот метод облегчает предоставление сервисов анализа ПДн, не внося риск злоупотребления ПДн и не ставя под угрозу точность алгоритмов «добычи данных». Процесс управления запросами следует использовать для обеспечения уверенности в обработке только достаточного количества ПДн для задействованных процессов.

Методы управления запросами включают в себя ограничение объема результатов запроса, контроль за перекрытием последовательных запросов, ведение контрольных журналов всех запросов, на которые даны ответы, и постоянную проверку на предмет возможной компрометации, отбрасывания ячеек ПДн малого размера и кластеризации объектов во взаимоисключающие элементарные совокупности.

7.2.4.10 Инвентарная опись персональных данных

Общее описание

Компонент инвентарной описи ПДн предоставляет обзор ПДн, хранящихся в ИСПДн. Информация из системы классификации ПДн должна использоваться для классификации хранящихся в системе значений ПДн. Для определения субъекта ПДн, связанного с конкретным элементом ПДн, должна использоваться система управления идентификационными данными. Компонент инвентарной описи ПДн должен предоставлять заинтересованной в обеспечении безопасности ПДн стороне, использующей систему, по крайней мере, следующую метрику:

- количество ПДн в системе (количество записей);
- количество субъектов ПДн, предоставивших информацию.

В зависимости от требований защиты ПДн этот компонент может предоставлять дополнительную информацию, такую как список субъектов ПДн.

Компонент инвентарной описи ПДн выполняет сходную функцию у всех действующих субъектов — предоставляет обзор того, сколько ПДн хранится в определенном месте и кто является соответствующими субъектами ПДн. ИСПДн оператора должна расширять эти функциональные возможности путем ведения учета обработки ПДн, выполненной системами обработчиков ПДн. Это должно осуществляться во взаимодействии с соответствующими компонентами управления ПДн и архивирования ПДн в ИСПДн обработчика.

7.2.4.11 Раскрытие персональных данных

Оператор ПДн

Компонент раскрытия ПДн отвечает за управление любым раскрытием ПДн оператором. Это может включать подготовку ПДн перед тем, как они покинут ИСПДн оператора. Например, оператор ПДн может обезличивать ПДн, используя соответствующий компонент, перед отправкой их обработчику ПДн. Раскрытие ПДн часто требует использования компонента передачи ПДн.

Если при раскрытии ПДн используется обезличивание, журнал регистрации должен содержать описание функции обезличивания, используемой для раскрытия ПДн. В такой ситуации в случаях раскрытия следует использовать разные функции обезличивания, поскольку это уменьшает возможность связывания раскрытых баз данных друг с другом, так как один и тот же идентификатор не преобразуется в один и тот же псевдоним.

Обработчик ПДн

ПДн могут быть раскрыты системой персональных данных обработчика ПДн таким же образом, как и системой оператора ПДн. Любое такое раскрытие должно быть осуществлено в соответствии с указаниями оператора ПДн.

7.2.4.12 Архивирование и хранение персональных данных

Общее описание

Если ПДн не находятся в активном использовании и планируется архивирование, их следует подготовить к архивированию. Компонент архивирования и хранения должен обеспечивать уверенность в том, что архив имеет достаточную защиту и что соблюдаются процедуры архивирования и хранения. Шифрование, распределение секрета и обезличивание могут использоваться для обеспечения защиты архивированных ПДн от несанкционированного доступа. При этом необходимо обеспечить сохранение и защиту параметров данных методов, например ключей шифрования, схемы распределения секрета или параметров обезличивания, чтобы осуществить последующее восстановление ПДн.

Если срок хранения ПДн истекает, этот компонент должен запланировать обезличивание или безопасное удаление ПДн из системы.

7.2.4.13 Протоколирование

Компонент протоколирования должен фиксировать каждую транзакцию, осуществляемую с ПДн. Этот компонент должен быть интегрирован с каждым другим компонентом, чтобы он мог фиксировать все соответствующие действия.

Идентификационные данные действующего субъекта или субъектов, которые получают доступ к ПДн, инициируют транзакции с ПДн или получают ПДн в результате транзакций с ПДн, должны быть зафиксированы в журнале регистрации транзакций. Это предполагает интеграцию протоколирования

с аутентификацией, авторизацией и модулями уровня ПДн. Для предотвращения вмешательства в записи журнала регистрации следует использовать методы безопасного протоколирования.

7.2.4.14 Взаимосвязь между принципами обеспечения безопасности и компонентами на уровне персональных данных

Пример взаимосвязи между принципами обеспечения безопасности и компонентами на уровне персональных данных приведен в таблице 3. Обозначение «X» в таблице указывает на взаимосвязь между компонентом данного уровня и принципом, однако указанная взаимосвязь приводится только в качестве примера.

Таблица 3 — Пример взаимосвязи между принципами обеспечения безопасности и компонентами на уровне персональных данных

Компоненты	Принципы										
	Согласие и выбор	Законность цели и ее спецификация	Ограничение на сбор информации	Минимизация данных	Ограничения в отношении использования, хранения и раскрытия	Точность и качество	Открытость, прозрачность и уведомление	Индивидуальное участие и доступ	Ответственность	Обеспечение безопасности информации	Соответствие
Управление ПДн	X	X	X	X	X	—	X	X	—	—	—
Передача ПДн	X	X	—	X	X	—	X	X	—	—	—
Проверка правильности ПДн	—	—	—	—	—	X	—	—	—	—	—
Обезличивание ПДн	—	—	—	X	—	—	—	—	—	X	—
Распределение секрета	—	—	—	X	—	—	—	—	—	X	—
Шифрование ПДн	—	—	—	X	—	—	—	—	—	X	—
Использование ПДн	X	X	—	X	X	X	X	—	—	—	—
Безопасные вычисления	—	—	—	X	—	—	—	—	—	X	—
Управление запросами	—	—	—	X	X	—	—	—	—	X	—
Инвентарная опись ПДн	—	—	—	X	X	—	X	—	X	—	—
Раскрытие ПДн	X	X	—	X	X	—	X	—	—	—	—
Архивирование и хранение ПДн	X	X	—	X	X	—	X	—	—	—	—
Протоколирование	—	—	—	—	—	—	—	—	X	X	—

7.3 Представление с точки зрения действующих субъектов (сторон)

7.3.1 Общие положения

Представление с точки зрения действующих субъектов (сторон) иллюстрирует, как компоненты базовой архитектуры реализуются в системах ПДн конкретной стороны, заинтересованной в обеспечении безопасности ПДн. Для каждого действующего субъекта представление определяет подмножество компонентов, пригодных для реализации в ИСПДн действующего субъекта. Разработчик использует это представление для принятия решения о том, какие компоненты должны быть включены в архитектуру ИСПДн стороны, заинтересованной в обеспечении безопасности ПДн.

Это представление не определяет ни один из компонентов ИСПДн конкретной стороны как обязательный.

7.3.2 Система субъекта персональных данных

ИСПДн субъекта ПДн сосредоточивается (но не ограничивается) на вопросах доведения политики обеспечения безопасности ПДн, управления согласиями и сбора ПДн.

Поскольку субъект ПДн является стороной, предоставляющей ПДн всем системам, то используемая субъектом ИСПДн должна содержать компоненты для обеспечения безопасности ПДн во время сбора. Эти методы могут включать (но не ограничиваться) обезличивание, шифрование и распределение секрета.

Архитектура ИСПДн субъекта представлена на рисунке 2.



Рисунок 2 — Архитектура информационной системы персональных данных субъекта персональных данных

7.3.3 Система оператора персональных данных

ИСПДн оператора должна доводить политику защиты персональных данных всем остальным участникам. Кроме того, оператор ПДн должен управлять сбором и обработкой всех ПДн. ИСПДн оператора должна обрабатывать ПДн на основе актуальной политики, требований защиты ПДн и любых предпочтительных способов защиты, которые были получены от субъекта ПДн. Оператор ПДн должен убеждаться в том, что компоненты установок Обеспечение безопасности ПДн все время содержат актуальную информацию о политике и целях.

Кроме того, оператор управляет обработкой ПДн обработчиками ПДн. Это включает надзор и ответственность за обеспечение соблюдения применимых политик обеспечения безопасности ПДн, а также любых ограничений, связанных с согласием и основными способами защиты, которые были получены от субъекта ПДн. Это требует от оператора ПДн передачи этой информации обработчикам ПДн, контроля проводимых ими мероприятий и принятия корректирующих мер, если ограничения не соблюдаются.

Кроме того, оператор ПДн может применять технологии, улучшающие (обеспечивающие) конфиденциальность персональных данных, такие как обезличивание или распределение секрета с целью дополнительного уменьшения вероятности того, что ИСПДн обработчика может определить субъекта ПДн. Архитектура ИСПДн оператора ПДн приведена на рисунке 3.



Рисунок 3 — Архитектура информационной системы персональных данных оператора персональных данных

7.3.4 Система обработчика персональных данных

Обработчик ПДн использует свою ИСПДн для обработки ПДн в соответствии со своим соглашением с оператором ПДн. Система оператора ПДн передает информацию о политике и предпочтительных способах защиты, связанных с ПДн и необходимых для их обработки. Кроме того, система обработчика ПДн должна быть способна поддерживать ПДн, преобразованные с помощью технологий, улучшающих (обеспечивающих) конфиденциальность ПДн.

Если для обеспечения защиты ПДн используются технологии, улучшающие обеспечение безопасности ПДн, которые не меняют представление ПДн (например, обезличивание), то ИСПДн обработчика не должна содержать специальных технологий обработки. Однако, если используются криптографические методы, такие как распределение секрета или шифрование ПДн, система обработчика ПДн должна использовать безопасные многосторонние вычисления или процедуру расшифрования ПДн. Безопасные многосторонние вычисления могут предлагать возможность снижения риска нарушения безопасности ПДн во время обработки. Архитектура ИСПДн обработчика ПДн приведена на рисунке 4.



Рисунок 4 — Архитектура информационной системы персональных данных обработчика персональных данных

7.4 Представление с точки зрения взаимодействия

7.4.1 Общая информация

Представление с точки зрения взаимодействия описывает, как взаимодействуют компоненты, реализованные в ИСПДн различных сторон, заинтересованных в обеспечении безопасности ПДн. Большинство компонентов, представленных в данной базовой архитектуре, требует обмена информацией или взаимодействия между действующими субъектами. В данном подразделе приведены описания компонентов, которые могут принимать участие в обмене ПДн между действующими субъектами. Разработчик системы может использовать это представление для проектирования взаимодействия между ИСПДн отдельных действующих субъектов.

Для каждого уровня компонентов архитектуры представлен рисунок. На рисунке показано распределение компонентов среди действующих субъектов (см. рисунки 5, 6 и 7). Если один компонент охватывает несколько действующих субъектов, то данные или программный код этого компонента должны совместно использоваться соответствующими действующими субъектами. Следует обратить внимание на то, что это не означает, что все ПДн должны быть совместно используемыми. Информация должна распространяться только по принципу наименьшего уровня привилегий — если действующему субъекту не требуется определенная информация для выполнения его обязанностей, он не должен получать доступ к этой информации. Например, даже если ИСПДн обработчика требует доступа к основным способам обеспечения безопасности ПДн субъекта, чтобы соблюдать их, она должна иметь доступ только к предпочтительным способам защиты тех субъектов ПДн, для которых ей предоставляли ПДн. Оператор может получать ПДн от многих субъектов, но, если оператор не делегирует обработку от имени конкретного субъекта ПДн обработчику, он не должен передавать соответствующие предпочтительные способы защиты. С другой стороны, если ПДн передаются от оператора обработчику, предпочтительные способы защиты соответствующих субъектов ПДн должны предоставляться ИСПДн обработчика.

7.4.2 Уровень установок

Уровень установок содержит сервисы и информацию, регулирующую все аспекты обработки ПДн. Соответственно, он должен участвовать во всей обработке ПДн. Распределение компонентов на уровне установок среди действующих субъектов приведено на рисунке 5.



Рисунок 5 — Распределение компонентов на уровне установок

7.4.3 Уровень управления идентификационными данными и управления доступом

Некоторые сервисы управления идентификационными данными являются общими и используются всеми действующими субъектами. Однако это не означает, что все действующие субъекты должны совместно использовать всю идентификационную информацию. Должен соблюдаться принцип наименьшего уровня привилегий, и каждая система персональных данных должна иметь доступ только к необходимой ей идентификационной информации. Распределение компонентов на уровне управления идентификационными данными и управления доступом приведено на рисунке 6.



Рисунок 6 — Распределение компонентов на уровне управления идентификационными данными и управления доступом

7.4.4 Уровень персональных данных

Уровень ПДн содержит общие используемые сервисы, такие как общее управление ПДн и инвентарная опись ПДн. Однако следует отметить, что на этом уровне имеются сервисы, которые могут быть реализованы для любого действующего субъекта, но в зависимости от проектирования системы их, может быть, целесообразно реализовывать только для некоторых действующих субъектов. Например, распределение секрета дает наибольший эффект при использовании непосредственно в системе персональных данных субъекта ПДн. Однако оно может также выполняться системой оператора ПДн перед передачей ПДн в систему обработчика ПДн. Возможный способ распределения компонентов на уровне ПДн приведен на рисунке 7.

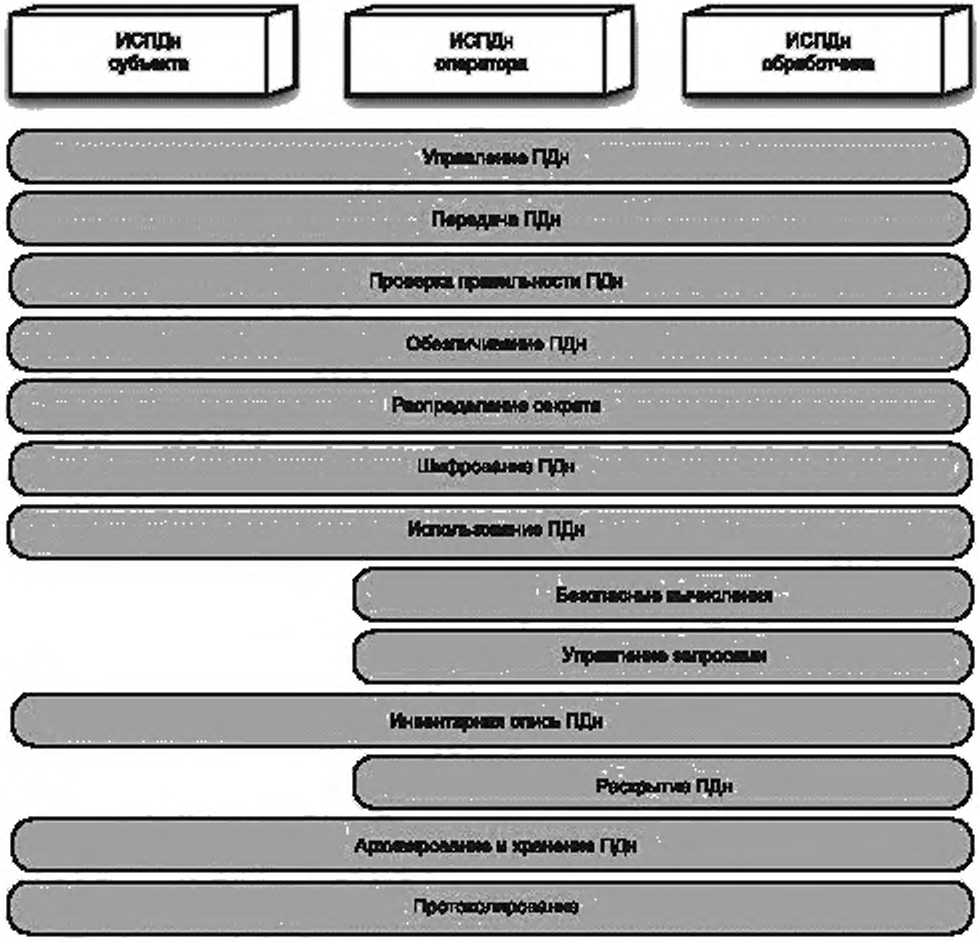


Рисунок 7 — Распределение компонентов на уровне персональных данных

Приложение А
(справочное)

Примеры значимых вопросов, связанных с защитой персональных данных

А.1 Общая информация

В данном приложении приведены примеры связанных с ПДн вопросов, значимых для архитектуры защиты ИСПДн. Значимые вопросы связаны с компонентами архитектуры защиты ПДн, при этом каждый компонент соответствует одному или нескольким значимым вопросам. Разработчикам следует идентифицировать конкретные значимые вопросы для их приложения и обеспечивать уверенность в том, что проектирование архитектуры защиты ИСПДн включает в себя компоненты, касающиеся значимых вопросов.

В приведенном ниже примере значимые вопросы уровня разбиваются на ряд подвопросов. Описанные здесь подвопросы приводятся в качестве иллюстрации и не обязательно являются полными. Разработчики должны определять соответствующие значимые вопросы и подвопросы для своего приложения в процессе анализа.

А.2 Получение и сообщение согласия

Согласие субъекта ПДн на обработку своих ПДн является важным аспектом управления ПДн. Соответственно, архитектура защиты ИСПДн должна включать в себя элементы, позволяющие осуществлять управление этим согласием в дополнение к элементам, обеспечивающим соблюдение ограничений такого согласия.

Согласие является характерным для заявленных целей использования и должно быть добровольно получено от субъекта ПДн на основе предоставленной оператором ПДн информации об этих целях и всех объектах (оператор ПДн и обработчик(и) ПДн), обрабатывающих ПДн, включая имеющие отношение к ним правовые основания.

В некоторых случаях применимое законодательство может определять исключения, когда обработка ПДн может быть разрешена без согласия субъекта ПДн (например, в связи с расследованием на законном основании). Для определения всех таких исключений и соответствующих положений о согласии необходимо обратиться к соответствующему законодательству.

Согласие может также предоставляться законным представителем (например, родитель, опекун, поверенный), если субъект ПДн не является правомочным с юридической точки зрения (например, субъект ПДн является ребенком). Представитель предоставляет ПДн субъекта ПДн вместо самого субъекта ПДн, а также определяет и предоставляет соответствующую информацию о согласии и ограничениях в отношении использования и передачи ПДн другим сторонам от имени субъекта ПДн. ПДн и связанная с ними информация о согласии и использовании должна конфиденциально храниться представителем.

Представителями должны быть доверенные лица, действующие в интересах своих клиентов. В случае воспринимаемого нарушения доверия представителем правовые санкции могут быть довольно ограниченными, особенно в ситуации близких отношений представителя с субъектом ПДн (например, родитель или опекун). В тех случаях, когда представителями являются специалисты (например, поверенные), назначенные для осуществления действий от имени субъектов ПДн, возможно обращение к правовым и профессиональным санкциям для решения вопроса в отношении представителей, которые не выполняют свои связанные с доверием обязанности.

К числу связанных с согласием значимых вопросов относится:

- получение согласия от субъекта ПДн или его представителя;
- безопасная передача и фиксирование информации о согласии;
- разрешение на отзыв или изменение согласия;
- связывание информации о согласии с ПДн;
- фиксирование заявления о согласии;
- реагирование на отзыв и изменение ранее данного согласия.

В тех случаях, когда субъект ПДн не дает согласия на сбор и обработку своих ПДн, может возникнуть необходимость в осуществлении альтернативных механизмов, не задействующих ПДн. В тех случаях, когда альтернативные механизмы недоступны, может возникнуть необходимость запретить субъекту ПДн пользоваться услугой.

А.3 Доведение целей сбора персональных данных

Операторы ПДн осуществляют сбор ПДн для определенной цели. Информация об этих целях должна быть представлена субъекту ПДн во время взаимодействия, когда требуется его согласие.

Информация о цели обработки должна сообщаться операторам ПДн или обработчикам ПДн всякий раз при передаче ПДн (например, путем маркировки ПДн с указанием цели перед передачей). Таким образом, все операторы ПДн и обработчики ПДн знают цель и пределы разрешенной обработки ПДн.

Обработка ПДн в соответствии с установленными целями может быть обеспечена посредством организационных мер. Альтернативным образом для обеспечения соблюдения пределов обработки ПДн могут использоваться технологии, улучшающие обеспечение безопасности ПДн, такие как управление запросами.

Некоторые из связанных с этим значимых вопросов для ИСПДн, поддерживающей и сообщающей информацию о целях сбора ПДн, включают в себя следующее:

- ввод и обновление информации, описывающей цель(и) сбора, использования и передачи ПДн;

- передача и представление информации, описывающей цель(и) сбора ПДн в ИСПДн;
- связывание информации о цели(ях) сбора с соответствующими ПДн;
- обеспечение уверенности в том, чтобы вся дальнейшая обработка не выходит за рамки указанной цели.

А.4 Безопасная обработка персональных данных

Разработчики ИСПДн должны учитывать характер и масштаб авторизованного доступа к ПДн. Чем чаще осуществляется доступ к ПДн и чем больше людей имеет права доступа к ПДн, тем выше вероятность нарушений безопасности ПДн.

Еще одним фактором, который необходимо учитывать, является уровень прямого контроля оператора ПДн или обработчика ПДн над обрабатываемыми ПДн. Например, если осуществляется удаленный доступ к ПДн в системе оператора ПДн или обработчика ПДн, этот субъект должен присвоить ПДн более высокий уровень риска.

Значимые вопросы для процессов передачи и хранения ПДн должны охватывать, по крайней мере, следующее:

- сбор и модификацию ПДн;
- авторизацию передачи ПДн;
- аутентифицированную и конфиденциальную передачу ПДн;
- хранение ПДн;
- управление доступом к ПДн;
- обеспечение уверенности в точности ПДн;
- применение дополнительных мер защиты и технологий, улучшающих конфиденциальность ПДн, которые рекомендованы в рамках обеспечения безопасности ПДн.

А.5 Классификация и контроль персональных данных

Интегральным компонентом оценки риска нарушения обеспечения безопасности ПДн должна быть разработка моделей потоков обработки ПДн. Блок-схема обработки ПДн должна не только показывать сферы сбора, передачи, использования, хранения или уничтожения ПДн, но также показывать сферы, где осуществляется обработка специальных категорий ПДн, требующих реализации более строгих мер защиты.

Классификация данных с отнесением их к ПДн и к не являющимся ПДн представляет собой минимальное требование при обработке специальных категорий ПДн (например, персональные данные о здоровье, этнической принадлежности и т. д.). Такие данные должны подлежать более строгим мерам защиты согласно соответствующему законодательству.

Значимые вопросы классификации и контроля в ИСПДн должны включать в себя следующее:

- определение того, какие данные относятся к ПДн,
- классификацию ПДн;
- определение числа действующих субъектов ПДн;
- определение количества и чувствительности ПДн;
- контроль передачи и внутреннего копирования ПДн.

А.6 Учет и аудит операций с персональными данными

Учет транзакций с использованием ПДн должен вестись в базе данных транзакций ПДн. Учет должен включать в себя фиксирование всей обработки ПДн и любых возникших ошибок, которые могли привести к компрометации конфиденциальности или целостности ПДн. Учетные записи должны подвергаться периодическому независимому аудиту для проверки на предмет возможных нарушений конфиденциальности и целостности, несанкционированного доступа или другого несанкционированного поведения.

Значимые вопросы, связанные с возможностью проведения аудита операций с ПДн, включают в себя следующее:

- регистрацию предоставления, изменения и отзыва согласия;
- регистрацию хранения и передачи ПДн;
- регистрацию обработки чувствительных ПДн;
- регистрацию передачи ПДн.

А.7 Архивирование и уничтожение персональных данных

Когда ПДн больше не требуются, их следует уничтожать. Процедуры уничтожения должны обеспечивать уверенность в том, что восстановление ПДн с носителя, используемого для их хранения, невозможно.

Значимые вопросы, связанные с надлежащим архивированием и уничтожением ПДн, включают в себя следующее:

- безопасное резервное копирование ПДн;
- методы безопасного уничтожения ПДн.

В таблицах А.1, А.2 и А.3 приведены примеры взаимосвязей между значимыми вопросами и компонентами уровней базовой архитектуры, определенной в настоящем стандарте. Обозначение «X» в таблице указывает на взаимосвязь между компонентом данного уровня и значимым вопросом, однако указанная взаимосвязь между значимыми вопросами и компонентами приводится только в качестве примера.

Таблица А.1 — Примеры взаимосвязи между значимыми вопросами и компонентами на уровне установок

Компоненты	Значимые вопросы						
	Получение и сообщение согласия	Поддержка информации о целях	Безопасное хранение и передача ПДн	Безопасная обработка ПДн	Классификация и контроль ПДн	Возможность проведения аудита операций с ПДн	Архивирование и уничтожение ПДн
Сообщение политики и целей	X	X	X	X	—	X	—
Классификация ПДн	—	—	X	X	X	X	X
Управление согласиями	X	—	—	—	X	X	—
Управление предпочтительными способами защиты	X	X	X	X	—	X	X

Таблица А.2 — Примеры взаимосвязи между значимыми вопросами и компонентами на уровне управления идентификационными данными и управления доступом

Компоненты	Значимые вопросы						
	Получение и сообщение согласия	Поддержка информации о целях	Безопасное хранение и передача ПДн	Безопасная обработка ПДн	Классификация и контроль ПДн	Возможность проведения аудита операций с ПДн	Архивирование и уничтожение ПДн
Управление идентификационными данными	X	—	X	—	X	X	X
Обезличивание	—	—	X	—	—	—	—
Управление доступом	—	—	X	X	—	X	—
Аутентификация	—	—	X	X	—	X	—
Авторизация	—	—	X	X	—	X	—

Таблица А.3 — Примеры взаимосвязи между значимыми вопросами и компонентами на уровне персональных данных

Компоненты	Значимые вопросы						
	Получение и сообщение согласия	Поддержка информации о целях	Безопасное хранение и передача ПДн	Безопасная обработкаПДн	Классификация и контроль ПДн	Возможность проведения аудита операций с ПДн	Архивирование и уничтожение ПДн
Управление ПДн	—	—	X	—	X	—	X
Передача ПДн	—	—	X	—	X	—	—
Проверка правильности ПДн	—	—	—	X	—	—	—
Обезличивание ПДн	—	—	X	—	—	X	—
Распределение секрета	—	—	X	—	—	—	—

Окончание таблицы А.3

Компоненты	Значимые вопросы						
	Получение и сообщение согласия	Поддержка информации о целях	Безопасное хранение и передача ПДн	Безопасная обработка ПДн	Классификация и контроль ПДн	Возможность проведения аудита операций с ПДн	Архивирование и уничтожение ПДн
Шифрование ПДн	—	—	X	—	—	—	X
Использование ПДн	—	—	—	X	—	—	—
Безопасные вычисления	—	—	—	X	—	—	—
Управление запросами	—	—	—	X	—	—	—
Инвентарная опись ПДн	—	—	—	—	X	X	X
Раскрытие ПДн	—	—	—	—	X	X	—
Архивирование и хранение ПДн	—	—	X	—	—	—	X
Протоколирование	—	—	—	—	X	X	X

А.8 Взаимосвязь с принципами обеспечения безопасности

В таблице А.4 приведен пример взаимосвязи между принципами обеспечения безопасности и значимыми вопросами, которые рассматриваются в данном приложении.

Таблица А.4 — Примеры взаимосвязи между принципами обеспечения безопасности и значимыми вопросами

Значимые вопросы	Принципы										
	Согласие и выбор	Законность цели и ее спецификация	Ограничение на сбор	Минимизация данных	Ограничения в отношении использования, хранения и раскрытия	Точность и качество	Открытость прозрачность и уведомление	Индивидуальное участие и доступ	Ответственность	Обеспечение безопасности информации	Соответствие
Получение и сообщение согласия	X	—	—	—	X	—	—	—	—	—	X
Сообщение целей сбора ПДн	—	X	—	—	—	—	X	—	—	—	X
Безопасная обработка ПДн	—	—	X	X	X	X	X	X	—	X	X
Классификация и контроль ПДн	—	—	—	—	—	—	—	—	X	X	X
Возможность проведения аудита операций с ПДн	—	—	—	—	—	—	—	—	X	X	X
Архивирование и уничтожение ПДн	—	—	—	—	X	—	—	—		X	X

Приложение Б
(справочное)

Система агрегирования персональных данных с безопасными вычислениями

Б.1 Общая информация

В данном приложении представлен пример архитектуры защиты ПДн, подготовленный на основе базовой архитектуры. Для минимизации раскрытия ПДн в архитектуре используются технологии, улучшающие конфиденциальность ПДн. Следует отметить, что этот пример приводится только с иллюстрационными целями. Любому приложению требуется архитектура, основанная на надлежащей оценке целей и соответствующих требований рассматриваемого приложения.

В приведенном примере описывается система, осуществляющая безопасный сбор ПДн у субъектов ПДн по защищенным каналам. Затем оператор ПДн использует распределение секрета для преобразования ПДн в информацию, не являющуюся ПДн. Результирующая информация, не являющаяся ПДн, передается трем обработчикам ПДн, которые используют безопасные вычисления для обработки ПДн, прошедших распределение секрета, не имея возможности связывать значения с отдельными субъектами ПДн. Узлы обработчика ПДн, участвующие в безопасных вычислениях, получают результат с распределением секрета и передают его аналитику данных, который может восстановить результат из полученных частей.

Б.2 Цель, действующие субъекты и размещение

Целью ИСПДн является сбор персональной информации у ряда субъектов ПДн. Сбор осуществляет организация, проводящая статистическое исследование. Однако, поскольку сама организация не обладает знаниями, необходимыми для статистического анализа, она привлекает для планирования и выполнения исследования и анализа данных внешнего аналитика данных.

Для обеспечения дополнительной защиты ПДн используются распределение секрета и безопасные многосторонние вычисления. Использование распределения секрета и безопасных многосторонних вычислений в этом сценарии требует участия, по крайней мере, трех организаций в безопасной обработке ПДн. Эти организации становятся узлами безопасных многосторонних вычислений, и их роль состоит в том, чтобы хранить ПДн, обработанные с применением метода распределения секрета, и осуществлять с ними безопасные многосторонние вычисления.

Если никакая из организаций, где размещен узел безопасных многосторонних вычислений, не публикует базу данных своей части, восстановление исходных ПДн другими узлами безопасных многосторонних вычислений невозможно. Узлы безопасных многосторонних вычислений обычно подбираются так, чтобы это были представители заинтересованных сторон, не вступающие в сговор.

Действующими субъектами приложения являются:

- физические лица, предоставляющие ПДн, которые являются субъектами ПДн;
- координатор исследования выступает в качестве оператора ПДн;
- узлы безопасных многосторонних вычислений и аналитик данных являются обработчиками ПДн.

ИСПДн размещена, как приведено на рисунке Б.1:

- ИСПДн субъекта ПДн представляет собой веб-приложение, запускаемое в веб-браузере субъекта. Оно размещается на веб-сервере оператора ПДн;
- ИСПДн оператора представляет собой веб-приложение, размещенное на веб-сервере оператора ПДн;
- ИСПДн обработчика ПДн представляет собой специализированное приложение с подключенной системой безопасных вычислений для хранения данных с распределением секрета, отправленных на обработку.

Реализация системы безопасных вычислений приведена на рисунке Б.1.

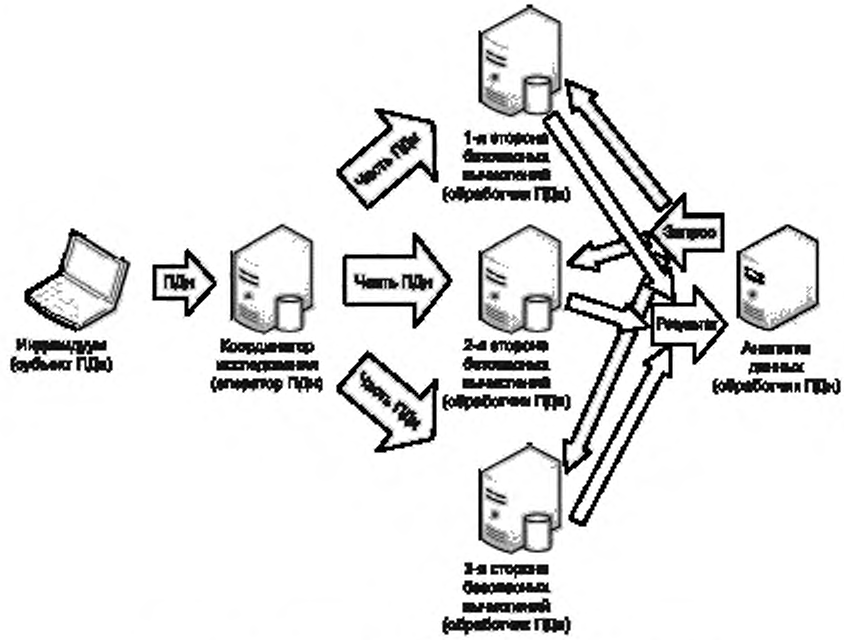


Рисунок Б.1 — Реализация системы безопасных вычислений

Б.3 Архитектура приложения ввода персональных данных

Координатор исследования подготавливает ИСПДн субъекта ПДн, которая содержит все три уровня архитектуры в соответствии с настоящим стандартом. Архитектура приложения ввода ПДн приведена на рисунке Б.2.



Рисунок Б.2 — Архитектура приложения ввода персональных данных

Компоненты могут быть реализованы описанным ниже образом.

Уровень установок:

- классификация ПДн: поскольку у субъекта ПДн запрашиваются специальные категории ПДн, вся вводимая ПДн автоматически считается чувствительной, за исключением факта и времени согласия;

- управление согласиями: после представления политики и цели приложение ввода ПДн в прямой форме запрашивает согласие субъекта ПДн перед представлением ему формы ввода ПДн. Решение о согласии и дата получения согласия также передаются в ИСПДн оператора. ИСПДн субъекта генерирует случайное значение и передает его в систему оператора ПДн вместе с согласием, чтобы сделать возможным изменение или отзыв согласия. Для изменения или отзыва согласия субъект ПДн обращается к координатору исследования и представляет случайное значение, которое может быть использовано для поиска ранее предоставленных ПДн и маркировки их для изменения или удаления;

- сообщение политики и целей: информация о политике обеспечения безопасности ПДн и цели сбора ПДн предоставляется субъекту ПДн в приложении ввода ПДн, когда оно загружается с веб-сервера.

Уровень управления идентификационными данными и управления доступом:

- система управления идентификационными данными: субъекты ПДн не идентифицируются, так как ввод данных осуществляется анонимно. Идентификационные данные оператора ПДн передаются через приложение ввода ПДн;

- управление доступом, аутентификация и авторизация: доступ к приложению ввода ПДн управляется путем ограничения его поставки с сервера оператора ПДн. Субъекты ПДн не аутентифицируются для сохранения анонимности (также не используется никакой метод групповой аутентификации). Субъекты ПДн аутентифицируют серверы оператора ПДн через стандартное безопасное HTTP соединение.

Уровень персональных данных:

- управление ПДн: приложение ввода ПДн не обеспечивает локальное хранение в веб-браузере субъекта ПДн. Оно сразу передает ПДн оператору ПДн;

- передача ПДн: для передачи ПДн на серверы оператора ПДн используется безопасное HTTP соединение;

- проверка правильности ПДн: полям в форме ввода ПДн присваиваются значения метаданных, которые используются для подтверждения того, что введенные значения соответствуют правильному формату;

- шифрование ПДн: шифрованием ПДн (и остальных сообщений между субъектом ПДн, оператором ПДн, контроллером) управляет безопасное HTTP соединение;

- инвентарная опись ПДн: после заполнения формы приложение ввода ПДн предоставляет возможность субъекту ПДн просматривать ответы и сохранять или печатать копию ПДн с использованием названия организаций оператора ПДн и обработчиков ПДн и случайной величины, отправленной вместе с согласием.

Б.4 Архитектура приложения управления исследованием

Оператор ПДн также использует ИСПДн в среде Интернет с некоторыми дополнительными возможностями для обработки ПДн, полученных от нескольких субъектов ПДн, передачи их обработчикам ПДн и проведения более тщательных аудитов. Архитектура ИСПДн координатора исследования представлена на рисунке Б.3.



Рисунок Б.3 — Архитектура информационной системы персональных данных координатора исследования

Компоненты могут быть реализованы следующим образом.

Уровень установок:

- сообщение политики и целей: оператор ПДн сообщает политику и цель субъекту ПДн, подготавливая и предоставляя приложение ввода ПДн. Оператор ПДн сообщает политику обработчикам ПДн посредством договоров;

- классификация ПДн: ИСПДн оператора ПДн содержит встроенные правила классификации ПДн, поступающих от субъектов ПДн, как чувствительных данных (за исключением информации о согласии);

- управление согласиями: оператор ПДн получает информацию о согласии из приложения ввода ПДн и хранит ее вместе с ПДн. Соответственное случайное значение может быть впоследствии использовано для осуществления изменения или отзыва согласия.

Уровень управления идентификационными данными и управления доступом:

- система управления идентификационными данными: никакая идентификационная информация субъекта ПДн не хранится. ИСПДн оператора дополнительно хранит информацию об узлах безопасных многосторонних вычислений и аналитике данных;

- управление доступом, аутентификация и авторизация: управление доступом к приложению ввода ПДн осуществляется путем разрешения или блокирования его поставки и блокирования сервиса сбора ПДн. Для авторизации доступа к ИСПДн оператора ПДн используются стандартные технологии (смарт-карты, биометрические данные, пароли и т. д.).

Уровень персональных данных:

- управление ПДн: ИСПДн координатора исследования получает ПДн от приложений ввода ПДн и хранит ее в базе данных. Система способна передавать ПДн в ИСПДн обработчика ПДн;
- передача ПДн: ИСПДн может получать безопасные HTTP-запросы от приложения ввода ПДн. Она может также открывать безопасные каналы к системам обработчика ПДн для передачи частей ПДн;
- распределение секрета: для передачи ПДн в систему безопасных вычислений ИСПДн использует распределение секрета для разделения индивидуальных значений на части. Каждая часть в отдельности не раскрывает информацию о введенных значениях;
- шифрование ПДн: шифрование используется при передаче ПДн из приложения ввода ПДн. Кроме того, части ПДн шифруются при передаче обработчикам ПДн. Следует отметить, что, поскольку распределение секрета обеспечивает конфиденциальность ПДн во время хранения, нет необходимости в шифровании частей ПДн;
- инвентарная опись ПДн: система может обеспечивать данные о количестве субъекту ПДн, предоставляющих ПДн для исследования;
- архивирование и хранение ПДн: после завершения исследования содержимое базы данных исследования безопасным образом архивируется. Для резервного копирования используются специальные инструменты системы управления базами данных;
- протоколирование: ИСПДн регистрируют каждую полученную запись ПДн, каждое действие, выполняемое оператором ПДн с использованием своей системы, и каждую передачу ПДн обработчикам ПДн.

Б.5 Архитектура безопасности приложения анализа персональных данных

ИСПДн аналитика данных представляет собой распределенную систему, состоящую из системы безопасного хранения и безопасных многосторонних вычислений и клиентского приложения для осуществления запросов к системе безопасных вычислений. Нижеприведенная архитектура охватывает всю распределенную систему. Следует отметить, что в представленном ниже описании архитектуры узел безопасных многосторонних вычислений означает программное обеспечение системы безопасных вычислений, запускаемое организациями, где размещается система безопасных многосторонних вычислений. Архитектура безопасности приложения анализа ПДн приведена на рисунке Б.4.



Рисунок Б.4 — Архитектура безопасности приложения анализа персональных данных

Компоненты могут быть реализованы следующим образом.

Уровень установок:

- сообщение политики и целей: аналитик данных и узлы безопасных многосторонних вычислений получают информацию о политике и цели с договором на анализ от оператора ПДн;
- классификация ПДн: информация, хранящаяся с использованием распределения секрета, классифицируется как ПДн и обрабатывается с применением безопасных многосторонних вычислений. Информация, не являющаяся ПДн, если таковая имеется, обрабатывается с использованием стандартных методов;
- управление согласиями: координатор исследования обеспечивает уверенность в том, что он передает ПДн, только давших согласие субъекту ПДн обработчикам ПДн. Если субъект ПДн изменяет или отзывает согласие, координатор исследования уведомляет аналитика данных и узлы безопасных многосторонних вычислений, которые затем должны удалить соответствующие части из своих систем.

Уровень управления идентификационными данными и управления доступом:

- система управления идентификационными данными: защита безопасных многосторонних вычислений зависит от узлов безопасных многосторонних вычислений, знающих идентификационные данные друг друга и

заинтересованных в защите персональных данных сторон, которые используют системы персональных данных (система координатора исследования, предоставляющая ПДн, и система анализа данных, делающая запросы). Аналогичным образом система персональных данных аналитика данных должна знать идентификационные данные узлов безопасных многосторонних вычислений и координатора исследования;

- управление доступом, аутентификация и авторизация: узлы безопасных многосторонних вычислений аутентифицируют и авторизуют систему персональных данных координатора исследования перед принятием ПДн от нее. Аналогичным образом узлы безопасных многосторонних вычислений аутентифицируют и авторизуют ИСПДн аналитика данных перед принятием запросов. ИСПДн аналитика данных использует стандартные методы для аутентификации и авторизации обработчика ПДн.

Уровень персональных данных:

а) управление ПДн: узлы безопасных многосторонних вычислений хранят ПДн в форме с распределением секрета. Система аналитика данных должна быть способна хранить запросы и их результаты;

б) инвентарная опись ПДн: узлы безопасных многосторонних вычислений могут предоставлять информацию о количестве записей в их базе данных с распределением секрета;

в) использование ПДн: аналитик данных формирует запросы и отправляет их узлам безопасных многосторонних вычислений. Узлы безопасных многосторонних вычислений обрабатывают ПДн, обеспечивая их защиту, и возвращают результаты запроса аналитику данных. Анализ данных составляет отчеты для координатора исследования;

г) передача ПДн: узлы безопасных многосторонних вычислений используют защищенные каналы для приема прошедших распределение секрета ПДн и запросов, а также для осуществления безопасных многосторонних вычислений. Результаты исследования передаются от аналитика данных координатору исследования, используя зашифрованные сообщения электронной почты;

д) распределение секрета: распределение секрета используется в системе безопасных многосторонних вычислений для хранения ПДн, а также в протоколах безопасных вычислений;

е) шифрование ПДн: шифрование используется при передаче ПДн и ПДн, прошедших распределение секрета, а также запросов и результатов. Результаты исследования опционально передаются в зашифрованном виде;

ж) управление запросами: узлы безопасных многосторонних вычислений отказываются отвечать на запросы, если количество записей ПДн меньше заранее определенного значения. Они также предоставляют аналитику данных только окончательные результаты статистических алгоритмов. Промежуточные значения хранятся в форме с распределением секрета. Используются только заранее согласованные статистические процедуры;

и) безопасные вычисления: эта система использует безопасные многосторонние вычисления с тремя узлами;

к) архивирование и хранение ПДн: в этом приложении узлы безопасных многосторонних вычислений должны архивировать свои базы данных в той же форме с распределением секрета или безопасно уничтожать ПДн. Аналитик данных безопасным образом архивирует результаты исследования. Журналы регистрации доступа и запросов также должны архивироваться и узлами безопасных многосторонних вычислений, и системой аналитика данных;

л) протоколирование: узлы безопасных многосторонних вычислений должны вести журнал регистрации всех следующих событий:

1) ПДн, полученные от координатора исследования,
2) запросы, полученные от аналитика данных,
3) результаты, возвращенные аналитику данных.

ИСПДн аналитика данных должна вести журнал регистрации всех сделанных запросов и всех полученных результатов.

Б.6 Заключение

Представленная архитектура показывает, как может быть создана защищенная ИСПДн при использовании технологий, улучшающих конфиденциальность персональных данных. Следует отметить, что использование различных парадигм безопасных вычислений может приводить к разной реализации и различным мерам защиты ПДн. В описанном в данной архитектуре решении используется система безопасных вычислений, напоминающая разработчику типичный механизм базы данных, что упрощает понимание системы.

Эта система имеет следующие функции безопасности, которые трудно обеспечить с помощью других методов:

- индивидуальные значения ПДн не заверяются никем, кроме субъекта ПДн;
- организаций, где размещаются базы данных вычислений частей ПДн значительно снижен риск атак со стороны нарушителей, так как базы данных частей информации не раскрывают никакие данные об индивидуальных значениях ПДн;
- если база данных какой-либо конкретной стороны скомпрометирована или похищена, то для вычисления новых частей ПДн можно использовать специальную процедуру многосторонних вычислений, называемую перераспределением, так чтобы даже при компрометации большего числа сторон риск для ПДн был минимальным.

Приложение В
(справочное)

Архитектура системы управления идентификационными данными и управления доступом, способствующая защите персональных данных

В.1 Общие положения

В данном приложении приведено описание примера архитектуры системы оценивания университетского курса обучения, которая позволяет студентам оценивать курс обучения, не раскрывая свою персональную информацию. Приложение способно аутентифицировать студентов, чтобы участие в оценке курса обучения могли принимать только имеющие на это право студенты, но идентификационные данные реального студента остаются неизвестными.

Примерная архитектура опирается на технологию мандатов на основе атрибутов, приведенную в ГОСТ Р 59382. Эта технология дает возможность владельцу мандата на основе атрибутов создать криптографическое свидетельство своего обладания определенными атрибутами (т. е. доказать, что он являются студентом университета и зарегистрирован на данный курс обучения).

В рассматриваемом примере университет берет на себя роль поставщика связанных с мандатами услуг [2] и выдает студенту сертифицированные мандаты, подтверждая правильность содержащихся в них ПДн. Получив такой мандат, студент может преобразовать содержащиеся в нем ПДн в новый токен доступа, содержащий обезличенные ПДн и соответствующее свидетельство, и представлять его приложению оценивания курса обучения, которое, в свою очередь, должно быть способно проверять достоверность полученного токена [3].

В.2 Цель, действующие субъекты и размещение

Цель этой системы состоит в том, чтобы дать возможность имеющим на это право студентам обезличено оценивать университетский курс обучения. В начале курса университет должен выпустить мандаты студентам, удостоверяющие внесение их в списки на текущий семестр и регистрацию на данный курс обучения. Кроме того, присутствие студентов на лекции также должно быть засвидетельствовано для каждой посещаемой лекции.

По окончании курса обучения студент может иметь возможность оценить курс, но сделать это анонимно. С другой стороны, университет хочет получать результаты оценивания только от студентов данного университета, которые зарегистрированы на этот курс обучения. Чтобы удовлетворить интересы обеих сторон, система оценивания курса обучения может принимать утверждения, создаваемые на основе мандата студента, будучи уверенной, что утверждения верны, но не идентифицируя при этом студента, стоящего за каждой оценкой.

Действующими субъектами в этой примерной архитектуре приложения являются:

- студент является субъектом ПДн, система студента имеет два основных сценария использования. Во-первых, она позволяет ему взаимодействовать со службой выпуска учетных данных университета, запрашивая выпуск учетных данных. Во-вторых, эти учетные данные могут позднее использоваться для генерации идентификационных утверждений о студенте, чтобы иметь возможность получения доступа к услуге, предлагаемой приложением оценивания курса обучения;
- служба выпуска мандатов университета действует как обработчик ПДн, так как она обрабатывает ПДн студентов, обращающихся с запросом на выпуск мандатов. Выпуск мандатов должен осуществляться с использованием специальной системы, доступной студенту либо через онлайновое приложение, либо через приложение, работающее в помещении службы выпуска мандатов университета. В последнем случае от студентов может требоваться представление своих ПДн в личном присутствии;
- приложение оценивания курса обучения — это предоставляемая университетом система, выполняющая функции оператора ПДн. Это приложение должно проверять утверждения, полученные от студентов, с целью одобрения или отклонения их доступа к оцениванию курса обучения. Чтобы одобрять или отклонять доступ к оцениванию курса обучения, эта система должна проверять аутентификационные свидетельства, представленные субъектом ПДн. В этом случае между приложением оценивания курса обучения и службой выпуска мандатов университета формируется доверенная взаимосвязь, так как приложение полагается на правильность информации мандатов, выпущенных службой выпуска мандатов университета.

В принципе, даже если одна организация (например, определенный факультет университета) управляет и выпуском мандатов, и оцениванием курса обучения, соответствующие действия, относящиеся к выпуску и представлению, не могут быть связаны с субъектом ПДн. В этом примере архитектура не включает в себя специальных обработчиков ПДн. На рисунке В.1 представлен обзор архитектуры — действующие субъекты и их взаимодействие.

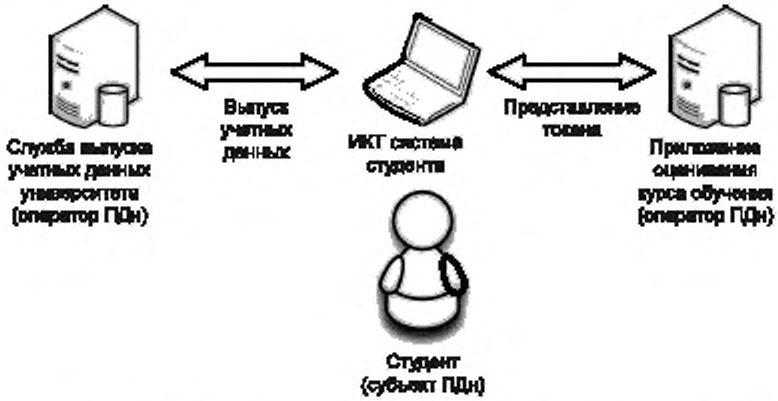


Рисунок В.1 — Обзор архитектуры — действующие субъекты и их взаимодействие[1)]

Служба выпуска мандатов университета должна быть способна выдавать студенту мандаты и гарантировать правильность ПДн, содержащихся в таких мандатах. Соответственно, служба выпуска мандатов университета может восприниматься как оператор ПДн, реагирующий на запросы субъекта ПДн о выдаче мандатов. Архитектура системы службы выпуска мандатов университета приведена на рисунке В.2.



Рисунок В.2 — Архитектура системы службы выпуска мандатов университета

Уровень установок:

- доведение политики и целей: система службы выпуска мандатов университета должна сообщать политику ИСПДн студенту, описывая ПДн, которые должны быть раскрыты студентом для выпуска мандатов. Кроме того, служба выпуска должна указывать цель такого сбора данных;
- управление согласиями: студент должен обратиться с запросом о выпуске учетных данных и дать согласие на обработку ПДн прежде, чем участвовать в протоколе выпуска.

Уровень управления идентификационными данными и управления доступом:

- система управления идентификационными данными: служба выпуска мандатов университета должна гарантировать правильность ПДн, содержащихся в мандатах. Для обеспечения доверия служба выпуска мандатов университета должна проводить проверку согласованности ПДн, которую пользователь раскрывает в ходе процесса до выдачи ему мандатов;
- управление доступом, аутентификация и авторизация: для того, чтобы служба выпуска учетных данных университета начала выпуск мандатов, она должна аутентифицировать студента. Кроме того, должна существовать соответствующая система управления доступом, которая обеспечивает безопасность путем ограничения доступа пользователей к системе выпуска мандатов.

Уровень персональных данных:

[1)] Указанные здесь потоки данных показывают только общий обзор архитектурной модели, но конкретное размещение может включать в себя дополнительные виды обмена данными.

- управление ПДн: служба выпуска учетных данных университета должна вести базу данных ПДн студентов с записями о зарегистрированных студентах, идентификационным номером студента, именем, датой рождения, выбранных им курсах обучения и других соответствующих ПДн. Эта информация должна быть в достаточной мере защищена, и должны существовать надлежащие механизмы управления, обеспечивающие уверенность в конфиденциальности ПДн;
- передача ПДн: при передаче таких ПДн, как мандаты, через Интернет ИСПДн службы выпуска мандатов университета должна быть способна создавать безопасные аутентифицированные соединения для защиты конфиденциальности ПДн и аутентификации намеченного получателя;
- инвентарная опись ПДн: служба выпуска учетных данных университета должна иметь базу данных с записями всех зарегистрированных студентов вместе с их ПДн, такими как идентификационный номер студента и контактная информация. Службы выпуска мандатов университета должна вести инвентарную опись учетных данных, выданных студентам, вместе с журналами регистрации транзакций для целей аудита. ИСПДн должна учитывать общее число полученных запросов, а также число успешных и неуспешных транзакций выпуска;
- протоколирование: служба выпуска учетных данных университета должна вести журнал регистрации транзакций для целей аудита.

В.3 Архитектура системы персональных данных студента

ИСПДн студента должна взаимодействовать с двумя другими системами. Если процесс выпуска мандатов является электронным, она должна запрашивать мандаты у службы выпуска мандатов университета. ИСПДн должна взаимодействовать с приложением оценивания курса обучения для оценки курса обучения.

Хотя студент должен аутентифицироваться при взаимодействии со службой выпуска мандатов университета, он может остаться анонимным при взаимодействии с приложением оценивания курса обучения. В последнем случае студент должен представлять доказательство обладания необходимыми привилегиями, а не раскрывать какие-либо ПДн. Система студента может быть комбинацией компонента хранения с высоким уровнем безопасности для хранения секретов, связанных с мандатами, и соответствующего программного компонента для взаимодействия с пользователем и связи с другими системами в этой архитектуре (см. рисунок В.3).



Рисунок В.3 — Архитектура системы персональных данных студента

Уровень установок:

- доведение политики и целей: студент должен получать два вида политик: политику представления при взаимодействии с приложением оценивания курса обучения и политику выпуска при взаимодействии со службой выпуска мандатов университета. В обоих случаях система студента должна быть способна обращаться с соответствующими политиками представления и выпуска, а также со взаимосвязанной политикой обеспечения безопасности ПДн;
- управление согласиями: до передачи любых ПДн другим системам в данной архитектуре система студента должна запрашивать осознанное согласие студента.

Уровень управления идентификационными данными и управления доступом:

- система управления идентификационными данными: ИСПДн студента должна хранить информацию об учетных данных, которые имеются у субъекта;
- система обезличивания: по проекту в ИСПДн студента должна быть реализована систему обезличивания, совместимая с системой, которую поддерживает приложение оценивания курса обучения. Система студента должна обеспечивать использование единственного псевдонима для каждого курса обучения в приложении оценивания курса обучения, чтобы можно было обновлять оценку. Приложение оценивания курса обучения должно ограничивать создание студентом более чем одного псевдонима для каждого курса обучения, с тем чтобы воспрепятствовать представлению студентом более чем одной оценки;

- управление доступом, аутентификация и авторизация: ИСПДн студента должна аутентифицировать систему приложения оценивания курса обучения, используя взаимную аутентификацию. Система студента должна генерировать необходимые свидетельства для выполнения требований анонимной аутентификации для приложения оценивания курса обучения.

Уровень персональных данных:

- управление ПДн: ИСПДн студента должна быть способна хранить его мандаты в защищенном хранилище;
- передача ПДн: ИСПДн студента должна быть способна обрабатывать мандаты, находящиеся во внешнем хранилище, таком как аппаратные токены или онлайновые сервисы. В целом ПДн не передаются из ИСПДн студента в приложение оценивания курса обучения. Однако системе студента может требоваться раскрытие некоторых ПДн службе выпуска мандатов университета при запросе о выпуске учетных данных;
- обезличивание ПДн: ИСПДн студента должна обеспечивать возможность создания токенов, привязанных к единственному псевдониму на каждый курс обучения;
- шифрование ПДн: ИСПДн студента должна быть способна осуществлять необходимые криптографические операции, которые обезличивают ПДн, содержащиеся в мандатах, до раскрытия их приложению оценивания курса обучения. В то же время для убеждения приложения оценивания курса обучения в правильности утверждений студентов должны использоваться мандаты на основе атрибутов;
- инвентарная опись ПДн: ИСПДн студента должна хранить учетные данные, принадлежащие студенту, в специальном хранилище, которым может быть смарт-карта или онлайновый сервис. Система может вести список учетных данных, которыми владеет студент. Эти учетные данные привязаны к определенному секрету, который используется для генерации необходимых криптографических свидетельств, требующих безопасного хранения (например, с использованием аппаратного токена).

В.4 Архитектура приложения оценивания курса обучения

Приложение оценивания курса обучения может использоваться для сбора отзывов о курсах обучения университета. Эта система должна взаимодействовать с системой студента и полагаться на правильность информации, содержащейся в мандатах, выданных службой выпуска мандатов университета.

Взаимодействие системы студента и приложения оценивания курса обучения начинается, когда студент принимает решение оценить курс обучения университета. ИСПДн студента должна направить запрос приложению оценивания курса обучения, которое, в свою очередь, должно ответить представлением политики, в которой указывается, что студент должен представить свидетельство того, что он является студентом университета, зарегистрировался на указанный курс обучения и посетил минимальное число лекций. Система студента должна использовать хранящиеся мандаты для генерации запрошенного свидетельства и представить их приложению оценивания курса обучения, которое, в свою очередь, проверяет представленные утверждения, не идентифицируя студента. Если проверка завершается успешно, студент считается имеющим право и получает доступ к форме оценивания курса обучения (см. рисунок В.4).



Рисунок В.4 — Архитектура приложения оценивания курса обучения

Уровень установок:

- доведение политики и целей: приложение оценивания курса обучения должно представить ссылку на свою политику защиты персональных данных системе студента. Эта политика должна определять, какие ПДн подтверждают утверждение во время анонимной аутентификации. Система студента должна обеспечить прочтение студентом этой политики;
- управление согласиями: приложение оценивания курса обучения должно получить осознанное согласие студента, чтобы продолжать процесс аутентификации и оценивания курса обучения. Приложение оценивания курса обучения должно быть способно фиксировать факт предоставления согласия.

Уровень управления идентификационными данными и управления доступом:

- система управления идентификационными данными: приложение оценивания курса обучения должно хранить свидетельства, представленные студентом. Это включает информацию о видах мандатов, идентификаторах мандатов и других генерируемых пользователем криптографических свидетельствах. Эта информация может использоваться для целей неотказуемости и надлежащей обработки предыдущих утверждений в случае повторного оценивания (например, когда студент хочет обновить представление). Студент по-прежнему остается анонимным, но различные оценки могут связываться между собой;

- система обезличивания: приложение оценивания курса обучения должно поддерживать использование псевдонимов, которые обеспечивают контролируемую связываемость студентов, но не раскрывают никакие ПДн студента вне его псевдонима. Приложение оценивания курса обучения должно взаимодействовать с системой студента для согласования схемы обезличивания, которую поддерживают обе системы;

- управление доступом, аутентификация и авторизация: приложение оценивания курса обучения должно проверять свидетельство, представленное системой студента. Аутентификация студента должна осуществляться анонимно на основе доверия, имеющегося у приложения оценивания курса обучения к точности ПДн, содержащейся в учетных данных, выданных службой выпуска учетных данных университета.

Уровень персональных данных:

- протоколирование: приложение оценивания курса обучения должно вести журналы регистрации осуществляемых транзакций для целей аудита. Оно также должно хранить список полученных криптографических материалов, таких, например, как ключи.

В.5 Заключение

Данный пример архитектуры, приведенный в настоящем стандарте, представляет приложение оценивания курса обучения, которое аутентифицирует студентов, не требуя от них раскрытия ПДн. Эта архитектура может быть далее расширена и адаптирована для других сценариев, где требуется аналогичная аутентификация. Архитектура основана на свойствах и концепциях мандатов на основе атрибутов, которые делают возможной аутентификацию, способствующую защите ПДн, обеспечивая при этом отсутствие связываемости и прослеживаемости для субъекта ПДн.

Приведенный пример представляет собой также пример шаблона архитектуры, который может быть воспроизведен для различных приложений. Архитектура состоит из компонентов, описанных в основной части настоящего стандарта, таких как менеджмент согласия, менеджмент идентификационных данных и аутентификация.

Эта архитектура обеспечивает следующие общие преимущества:

- отсутствие связи между выпуском и представлением мандатов;
- безопасную, но анонимную аутентификацию субъекта ПДн;
- контролируемую связываемость, когда это желательно;
- устранение необходимости раскрытия ПДн во время аутентификации и уменьшение таким образом потребности в дополнительных компонентах защиты.

Технологии, опирающиеся на концепции мандатов на основе атрибутов, могут также обеспечивать дополнительные функции, такие как контролируемая анонимность, минимальное раскрытие информации и отзыв мандатов в случае злоупотребления.

Библиография

[1] Федеральный закон от 27 июля 2006 г. № 152-ФЗ (в редакции от 30 декабря 2020) «О персональных данных»

[2] ИСО/МЭК 29115:2013 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к аутентификации сущности (Information technology — Security techniques — Entity authentication assurance framework)

[3] ABC4Trust «D2.1 Architecture for Attribute-based Credentials»

УДК 006.34:004.056:004.056.5:004.056.53:006:354 ОКС 35.030

Ключевые слова: архитектура защиты, персональные данные, субъект персональных данных, оператор персональных данных, обработчик персональных данных

Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 24.05.2021. Подписано в печать 01.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,60.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва. Нахимовский пр-т. д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru

gost.e-ecolog.ru