ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 19086-4— 2020

Информационные технологии

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ

Структура соглашения об уровне обслуживания (SLA)

Часть 4

Компоненты информационной безопасности и защиты персональных данных

(ISO/IEC 19086-4:2019, Cloud computing — Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII, IDT)

Издание официальное

Москва
Стандартинформ
2020

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН) и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

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 10 ноября 2020 г. № 1040-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 19086-4:2019 «Облачные вычисления. Структура соглашения об уровне обслуживания (SLA). Часть 4. Компоненты безопасности и защиты персональных данных» (ISO/IEC 19086-4:2019 «Cloud computing — Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII», IDT).

ИСО/МЭК 19086-4 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).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

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

5 ВВЕДЕН ВПЕРВЫЕ

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

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

Содержание

Введение

Настоящий стандарт может использоваться любой организацией или физическим лицом, участвующими в создании, модификации или интерпретации соглашения об уровне обслуживания (SLA) для служб облачных вычислений, соответствующего требованиям ИСО/МЭК 19086 (все части). Облачное SLA обуславливает ключевые характеристики предоставляемых вычислительных услуг и служит основой взаимопонимания между поставщиками (CSP) и потребителями (CSC) облачных служб.

Настоящий стандарт основан на основополагающих концепциях и определениях, содержащихся в ИСО/МЭК 19086-1.

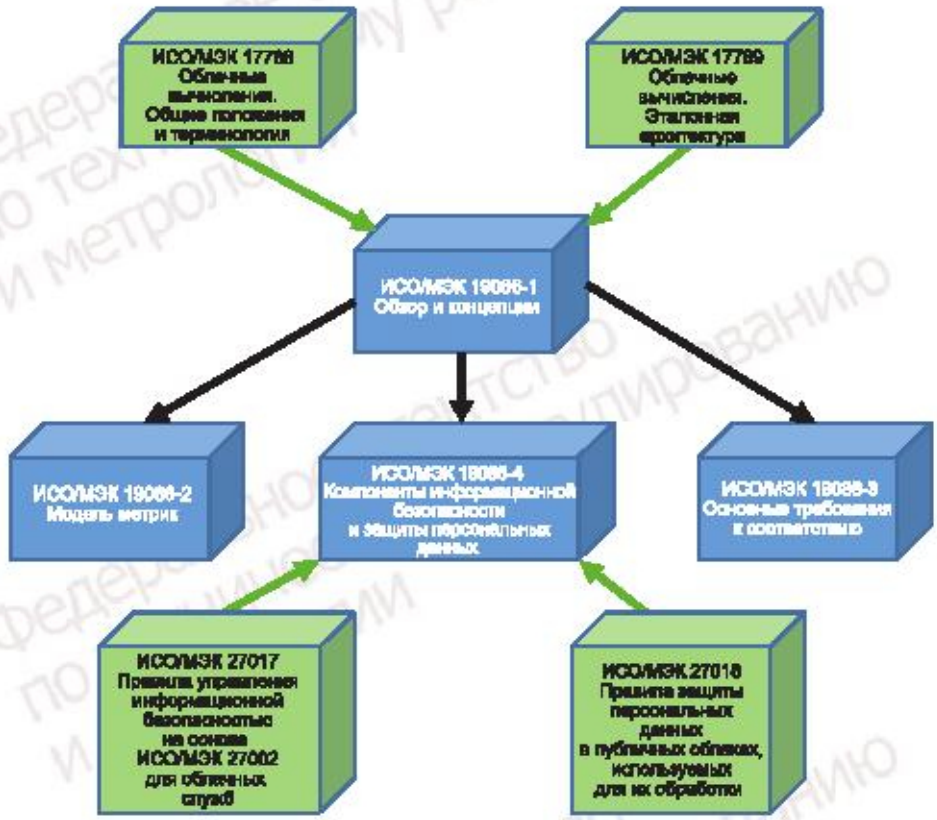

Рисунок 1 — Взаимосвязи между частями ИСО/МЭК 19086 и другими стандартами, относящимися к облачным вычислениям

На рисунке 1 представлен обзор содержания частей ИСО/МЭК 19086 и взаимосвязей между частями ИСО/МЭК 19086 и другими ключевыми стандартами, относящимися к облачным вычислениям.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ

Структура соглашения об уровне обслуживания (SLA)

Часть 4

Компоненты информационной безопасности и защиты персональных данных

Information technology. Cloud computing. Service level agreement framework (SLA). Part 4. Components of information security and of protection of PII

Дата введения — 2021—06—01

1 Область применения

Настоящий стандарт описывает компоненты обеспечения информационной безопасности и защиты персональных данных, а также целевые параметры уровня и качества обслуживания в соглашениях об уровне обслуживания облачных служб (облачное SLA), включая соответствующие требования и рекомендации.

Настоящий стандарт предназначен для использования как поставщиками, так и потребителями облачных служб.

2 Нормативные ссылки

В настоящем стандарте использованы следующие нормативные ссылки. Для датированных ссылок применяют только указанное издание, для недатированных — последнее издание (включая все изменения).

ISO/IEC 17788:2014, Information technology — Cloud computing — Overview and vocabulary (Информационные технологии. Облачные вычисления. Общие положения и терминология)

ISO/IEC 19086-1, Information technology — Cloud computing — Service level agreement (SLA) framework — Part 1: Overview and concepts (Информационные технологии. Облачные вычисления. Структура соглашения об уровне обслуживания (SLA). Часть 1. Обзор и концепции)

ISO/IEC 27017, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services (Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по управлению информационной безопасностью на основе ИСО/МЭК 27002 для облачных служб)

ISO/IEC 27018, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors» (Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки)

ISO/IEC 29100, Information technology — Security techniques — Privacy framework (Информационные технологии. Методы и средства обеспечения безопасности. Основы обеспечения приватности)

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 17788, ИСО/МЭК 19086-1, ИСО/МЭК 27017, ИСО/МЭК 27018 и ИСО/МЭК 29100.

Издание официальное

ИСО и МЭК поддерживают терминологические базы данных для использования в стандартизации в следующих адресах:

- платформа ИСО для онлайн-просмотра: доступна по адресу http://www.iso.org/obp
- МЭК Электропедия (IEC Electropedia): доступна по адресу http://www.electropedia.org/

4 Обозначения и сокращения

CSC — потребитель облачной службы (cloud service customer);

CSP — поставщик облачной службы (cloud service provider);

CSA — соглашение об облачной службе (cloud service agreement);

SLA — соглашение об уровне обслуживания (service level agreement);

Облачное SLA — соглашение об уровне обслуживания облачной службы (service level agreement);

SLO — целевые параметры уровня обслуживания облачной службы (cloud service level objective);

SQO — целевые параметры качества обслуживания облачной службы (cloud service qualitative objective);

VPN — виртуальная частная сеть (virtual private network);

ПДн — персональные данные (PII).

5 Взаимосвязь настоящего стандарта с другими частями ИСО/МЭК 19086

5.1 Общая информация

ИСО/МЭК 19086-1 содержит обзор, основополагающие концепции и определения структуры облачного SLA. В частности, определяются следующие фундаментальные понятия структуры облачного SLA:

- соглашение об облачной службе (CSA);
- соглашение об уровне обслуживания облачной службы (облачное SLA);
- целевые параметры уровня обслуживания облачной службы (SLO);
- целевые параметры качества обслуживания облачной службы (SQO).

ИСО/МЭК 19086-1 также описывает предметные области и компоненты, которые состоят из перечня SLO и SQO.

ИСО/МЭК 19086-2 содержит модель метрик, которая будет применяться для определения метрик, используемых в облачных SLA.

ИСО/МЭК 19086-3 содержит основные требования к соответствию, основанные на SLO и SQO, определенных в настоящем стандарте.

Настоящий стандарт основан на основополагающих концепциях и определениях компонентов информационной безопасности и защиты ПДн, приведенных в ИСО/МЭК 19086-1.

ИСО/МЭК 19086 (все части) предназначен содействовать установлению взаимопонимания между потребителями и поставщиками облачных служб. CSA и соответствующие облачные SLA различаются в зависимости от поставщиков облачных служб; кроме того, в некоторых случаях отдельные потребители облачных служб могут согласовывать разные условия для конкретной облачной службы с одним и тем же поставщиком. Настоящий стандарт призван помочь потребителям сравнивать облачные службы, предлагаемые разными поставщиками, с точки зрения информационной безопасности и защиты персональных данных. Для лучшего понимания облачных SLA настоящий стандарт следует использовать совместно с ИСО/МЭК 19086-1.

5.2 Соответствие требованиям

В разделе 5 ИСО/МЭК 19086-3:2017 установлены требования к соответствию облачных SLA в контексте ИСО/МЭК 19086-1. Настоящий стандарт применяет те же принципы в отношении соответствующих облачных SLA. В каждом из компонентов, указанных в настоящем стандарте, в областях обеспечения информационной безопасности (раздел 7) и защиты ПДн (раздел 8) описывается один или несколько SLO или SQO. При использовании одного из компонентов, приведенных в разделе 7 или 8, в соответствующем облачном SLA не требуется использовать SLO или SQO, описанные в этих компонентах. В соответствующем облачном SLA следует использовать SLO или SQO, определенные в настоящем стандарте, в зависимости от ситуации. Независимо от того, используется ли SLO или SQO, поставщик облачных служб должен использовать термины, определения, концепции и иные сущности таким

образом, чтобы они не противоречили соответствующим положениям ИСО/МЭК 19086-1 или настоящего стандарта.

ИСО/МЭК 19086-2 описывает модель определения метрик для соглашений об уровне обслуживания облачных служб (облачное SLA). При определении метрик SLO в соответствующих облачных SLA должна использоваться модель, приведенная в ИСО/МЭК 19086-2.

В соответствующем облачном SLA может использоваться подмножество компонентов, приведенных в настоящем стандарте (разделы 7 и 8), а также компоненты, выходящие за рамки настоящего стандарта. Однако соответствующее облачное SLA должно соответствовать определению терминов, компонентов или предметных областей, приведенных в настоящем стандарте и в ИСО/МЭК 19086-1, а также требованиям, установленным в настоящем стандарте. Если облачное SLA содержит определенный компонент или предметную область, то они должны соответствовать всем требованиям, указанным для такого компонента или предметной области. Для обеспечения соответствия настоящему стандарту не требуется внедрение каких-либо специальных технологий.

6 Обзор

6.1 Общая информация

Настоящий стандарт основан на основополагающих концепциях облачного SLA, общее описание которых содержится в ИСО/МЭК 19086-1. В описании каждого компонента соглашения, посвященного обеспечению информационной безопасности или защите ПДн, приводятся соответствующие SLO и SQO. В соответствии с ИСО/МЭК 19086-1 поставщик облачной службы может предоставлять более одного SLO и/или SQO.

Настоящий стандарт рассматривает требования конкретных компонентов и требования соответствия для SLO и SQO в области обеспечения информационной безопасности и защиты ПДн. Компоненты обеспечения информационной безопасности (см. 7.1—7.13) соответствуют структуре ИСО/МЭК 27002 и мерам обеспечения информационной безопасности в облачных средах, определенным в ИСО/МЭК 27017. Компоненты защиты ПДн (см. 8.1—8.9) соответствуют структуре ИСО/МЭК 29100 и мерам защиты ПДн в облачных средах, определенным в ИСО/МЭК 27018.

Поставщик облачной службы может определять SLO и SQO, используя описания SLO и SQO, приведенные в ИСО/МЭК 19086-1, и модель метрик, приведенную в ИСО/МЭК 19086-2. Затем потребитель облачной службы может установить свои требования к предоставляемым службам, используя те же SLO и SQO, что и поставщик. Это позволяет потребителю облачной службы напрямую сравнивать свои требования с возможностями поставщика и определять, какие возможности поставщика лучше всего соответствуют его требованиям. Дополнительные рекомендации по оценке SQO и SLO и принятию облачных SLA содержатся в ИСО/МЭК 19086-1:2016, подраздел 7.3.

6.2 Структура настоящего стандарта

Порядок следования разделов в настоящем стандарте не подразумевает их важности или приоритета. Каждый компонент облачного SLA, посвященный обеспечению информационной безопасности или защите ПДн, должен рассматриваться в соответствии с категориями, типами облачных возможностей и моделями развертывания облачных служб (см. ИСО/МЭК 17788).

Компоненты структурированы следующим образом:

1) Описание: описывается конкретный компонент. Приводится описание основных требований к соответствию и рекомендации по этим требованиям для каждого конкретного компонента.

2) Перечень SLO и SQO: описываются соответствующие SLO и SQO.

В ИСО/МЭК 19086-1 приведено следующее определение SLO: «обязательство поставщика службы облачных вычислений для конкретной количественной характеристики службы облачных вычислений, где значение представлено посредством интервальной или пропорциональной шкалы».

В ИСО/МЭК 19086-1 приведено следующее определение SQO: «обязательство поставщика службы облачных вычислений для конкретной качественной характеристики службы облачных вычислений, где значение представлено посредством номинальной или порядковой шкалы». Описание основных требований к соответствию и рекомендации по этим требованиям даны для каждого конкретного компонента.

3) Рекомендации: даются более подробные рекомендации для достижения целевых параметров уровня (SLO) и качества (SQO) обслуживания облачной службы. В отдельных случаях рекомендации

могут быть частично применимыми или недостаточными, а также могут не соответствовать конкретным требованиям SLO или SQO для поставщика облачной службы.

7 Компоненты обеспечения информационной безопасности

7.1 Компонент «Политики информационной безопасности»

7.1.1 Описание

Политики информационной безопасности устанавливают требования к обеспечению информационной безопасности и, при необходимости, описывают процедуры обеспечения безопасности при предоставлении, использовании и поддержке предоставляемых облачных служб.

Компонент «Политики информационной безопасности» должен задавать[1)] политику информационной безопасности, применяемую к предоставляемым[2)] облачным службам.

7.1.2 Целевые параметры качества обслуживания

Политики информационной безопасности

Положение, описывающее политики и процессы обеспечения информационной безопасности, реализуемые поставщиком для защиты предоставляемых облачных служб.

SQO «Политики информационной безопасности» должен описывать[3)] политику информационной безопасности, применяемую к предоставляемым облачным службам.

7.1.3 Рекомендации

Дополнительные сведения о политиках информационной безопасности приведены в ИСО/МЭК 27002 и ИСО/МЭК 27017.

Примечание — ИСО/МЭК 27017:2015 (5.1.1) определяет содержание типовой политики информационной безопасности.

7.2 Компонент «Организация деятельности по информационной безопасности»

7.2.1 Описание

Компонент «Организация деятельности по информационной безопасности» описывает разделение ролей и обязанностей между поставщиком и потребителем облачных служб.

Компонент «Организация деятельности по информационной безопасности» должен задавать роли и обязанности в отношении предоставляемых облачных служб.

7.2.2 Целевые параметры качества обслуживания

Разделение ролей и обязанностей

Разделение ролей и обязанностей между CSC и CSP.

В SQO «Разделение ролей и обязанностей» должны задаваться правила разделения ролей и обязанностей между CSC и CSP в отношении предоставляемых служб.

7.2.3 Рекомендации

Подробная информация о компоненте «Организация деятельности по информационной безопасности» приведена в ИСО/МЭК 27002 и ИСО/МЭК 27017.

7.3 Компонент «Менеджмент активов»

7.3.1 Описание

Компонент «Менеджмент активов» определяет предоставляемые активы и обязанности в отношении этих активов со стороны CSC и CSP. Активы могут включать в себя аппаратные средства, программное обеспечение и/или данные с позиций их принадлежности CSC и CSP.

---

1) Здесь и далее последний абзац описания компонента определяет назначение компонента в конкретном соглашении об уровне обслуживания. *Прим. перев.*

2) Здесь и далее под «предоставляемыми облачными службами» понимаются облачные службы, для которых заключено или заключается соглашение об уровне обслуживания. *Прим. перев.*

3) Здесь и далее второй абзац описания параметра уровня или параметра качества обслуживания определяет назначение соответствующего параметра в конкретном соглашении об уровне обслуживания. *Прим. перев.*

Компонент «Менеджмент активов» должен задавать активы и обязанности, связанные с этими активами, в отношении предоставляемых служб.

7.3.2 Целевые параметры уровня обслуживания

Частота обновления данных об активах

Максимальный интервал времени между обновлениями базы данных активов.

SLO «Частота обновления данных об активах» должен задавать максимальный интервал времени между обновлениями базы данных активов.

7.3.3 Целевые параметры качества обслуживания

Реестр активов и обязанностей

Перечень активов или категорий активов в облачном SLA, а также обязанностей и ответственности CSC и CSP по отношению к перечисленным активам или категориям активов.

SQO «Реестр активов и обязанностей» должен определять перечень активов и обязанностей CSC и CSP в отношении указанных активов для предоставляемых служб.

7.3.4 Рекомендации

В ИСО/МЭК 19944 можно найти дополнительные сведения о категориях типов данных в виде таксономии, с помощью которой можно описывать данные активы.

Дополнительные сведения, связанные с менеджментом активов, приведены в разделе 8 ИСО/МЭК 27017:2015.

7.4 Компонент «Управление доступом»

7.4.1 Описание

Компонент «Управление доступом» относится к мерам и средствам управления доступом, реализованным в предоставляемых облачных службах, в отношении доступа к самой службе, а также административного и делового доступа, описанных в ИСО/МЭК 17789.

Компонент «Управление доступом» должен задавать меры и средства разграничения доступа, реализованные в предоставляемых облачных службах.

7.4.2 Целевые параметры уровня обслуживания

7.4.2.1 Максимальное время, необходимое для аннулирования прав доступа пользователя

Максимальное время, необходимое для аннулирования прав доступа пользователя к предоставляемым службам.

SLO «Максимальное время, необходимое для аннулирования прав доступа пользователя» должен определять максимальное время, требуемое для аннулирования прав доступа пользователя к предоставляемым услугам.

7.4.2.2 Время аннулирования прав доступа пользователя в зависимости от уровня обязательств

Время, необходимое для аннулирования прав доступа пользователя к предоставляемым службам в виде указания минимально реализуемой доли от общего числа запросов на аннулирование доступа. Например, в течение двух часов должно быть выполнено минимум 95 % запросов на аннулирование прав доступа пользователей.

SLO «Время аннулирования прав доступа пользователя в зависимости от уровня обязательств» должен задавать нижнюю границу для доли запросов на аннулирование прав доступа пользователя, выраженную в процентах, которая должна быть выполнена в течение указанного промежутка времени.

7.4.3 Целевые параметры качества обслуживания

7.4.3.1 Регистрация и отмена регистрации пользователей

Описание процедур регистрации и отмены регистрации пользователей в предоставляемых облачных службах.

SQO «Регистрация и отмена регистрации пользователей» должен определять процедуры регистрации и отмены регистрации пользователей в предоставляемых облачных службах.

7.4.3.2 Экспертный анализ схем доступа

Описание возможностей поддержки экспертного анализа схем доступа в целях упреждающей идентификации и нейтрализации возможных угроз.

SQO «Экспертный анализ схем доступа» должен содержать описание возможностей поддержки экспертного анализа схем доступа в целях упреждающей идентификации и нейтрализации возможных угроз для предоставляемых служб.

7.4.3.3 Механизм аутентификации

Описание механизмов аутентификации, поддерживаемых поставщиком для предоставляемых облачных служб.

Описание механизмов аутентификации пользователей и администраторов, поддерживаемых поставщиком для предоставляемых облачных служб.

SQO «Механизм аутентификации» должен содержать описание механизмов аутентификации, которые могут быть использованы для предоставляемых служб.

7.4.3.4 Поддержка механизмов аутентификации третьей стороны

Описание поддерживаемых поставщиком облачной службы механизмов аутентификации третьей стороны.

SQO «Поддержка механизмов аутентификации третьей стороны» должен предоставлять описание механизмов аутентификации третьих сторон, которые могут быть использованы для предоставляемых служб.

7.4.3.5 Поддержка усиленной аутентификации

Описание механизмов усиленной аутентификации, используемых для контроля доступа потребителей облачной службы к предоставляемым службам. Например, с использованием многофакторной аутентификации.

SQO «Поддержка усиленной аутентификации» должен предоставлять описание механизмов усиленной аутентификации, которые могут использоваться для предоставляемых служб.

7.4.3.6 Поддержка анонимной аутентификации и аутентификации по псевдониму

Описание механизмов анонимной аутентификации и аутентификации по псевдониму, поддерживаемых для предоставляемых служб.

SQO «Поддержка анонимной аутентификации и аутентификации по псевдониму» должен предоставлять описание доступных механизмов анонимной аутентификации и аутентификации по псевдониму для предоставляемых служб.

7.4.4 Рекомендации

Руководство по управлению доступом к облачным службам содержится в ИСО/МЭК 27017 и ИСО/МЭК 27002.

Дополнительная информация об управлении доступом содержится в ИСО/МЭК 27002.

7.5 Компонент «Криптография»

7.5.1 Описание

Описание мер и средств криптографической защиты информации, предоставляемых поставщиком облачной службы своим потребителям. Меры и средства криптографической защиты информации предоставляются для трех состояний: передаваемые данные, хранимые данные и обрабатываемые данные.

Меры и средства криптографической защиты информации описаны в ИСО/МЭК 27002.

Компонент «Криптография» должен определять меры и средства криптографической защиты информации, связанные с представляемыми службами. Спецификация должна содержать идентификаторы используемых протоколов и алгоритмов, а также определение их криптографической стойкости, чтобы потребитель облачных служб мог сравнивать их между собой.

7.5.2 Целевые параметры качества обслуживания

7.5.2.1 Меры и средства криптографической защиты передаваемых данных

Описание мер и средств криптографической защиты передаваемых данных, связанных с представляемыми службами.

Примечание — Указанные меры и средства криптографической защиты обеспечивают конфиденциальность и целостность данных, передаваемых как внутри предоставляемых служб, так и между предоставляемыми службами, а также между потребителем облачной службы и предоставляемыми службами.

SQO «Меры и средства криптографической защиты передаваемых данных» должен описывать доступные криптографические средства защиты передаваемых данных.

7.5.2.2 Меры и средства криптографической защиты хранимых данных

Описание мер и средств криптографической защиты хранимых данных, связанных с представляемыми службами.

Примечание — Указанные меры и средства криптографической защиты обеспечивают конфиденциальность и целостность данных в процессе их хранения внутри предоставляемых служб.

SQO «Меры и средства криптографической защиты хранимых данных» должен описывать доступные криптографические средства защиты хранимых данных.

7.5.2.3 Меры и средства криптографической защиты обрабатываемых данных

Описание мер и средств криптографической защиты обрабатываемых данных, связанных с предоставляемыми службами.

Примечание — Указанные меры и средства криптографической защиты обеспечивают конфиденциальность и целостность данных в процессе их обработки внутри предоставляемых служб.

SQO «Меры и средства криптографической защиты обрабатываемых данных» должен описывать доступные криптографические средства защиты обрабатываемых данных.

7.5.2.4 Политика управления ключами

Описание политики управления ключами в предоставляемых службах, включающей в себя все доступные механизмы защиты ключей потребителей облачной службы от несанкционированного доступа со стороны поставщика облачных служб.

SQO «Политика управления ключами» должен предоставлять описание политики управления ключами для предоставляемых служб.

7.5.3 Рекомендации

Меры и средства криптографической защиты информации описаны в ИСО/МЭК 27002.

В ИСО/МЭК 27040 приведены определения передаваемых и хранимых данных.

7.6 Компонент «Физическая безопасность и защита от воздействия окружающей среды»

7.6.1 Описание

Компонент «Физическая безопасность и защита от воздействия окружающей среды» определяет процессы и меры, предпринимаемые поставщиком облачной службы, по защите физических объектов, используемых для предоставления соответствующих услуг, от потери данных, обеспечению возможности подключения и доступности необходимой инфраструктуры и ИТ-оборудования. Такие процессы и меры предназначены для защиты физических объектов от кражи, пожаров, наводнений, землетрясений, преднамеренного разрушения, неумышленного вреда, механических сбоев оборудования и перебоев питания.

К физическим объектам относятся стены и крыши зданий, оборудование инфраструктуры, например системы охлаждения, распределения питания, безопасности и противопожарной защиты, а также ИТ-оборудование, например серверы, оборудование для хранения данных и сетевое оборудование. К физическим объектам также относятся центры управления для мониторинга предоставляемых служб, в которых может осуществляться обработка данных потребителей и поставщиков облачных служб.

Компонент «Физическая безопасность и защита от воздействия окружающей среды» должен определять средства физической безопасности для предоставляемых служб.

7.6.2 Целевые параметры качества обслуживания

7.6.2.1 Мониторинг центров обработки данных

Положение о процессе мониторинга в центрах обработки данных, используемого при предоставлении соответствующих услуг. Этот процесс рассматривается в подразделе 9.4 ИСО/МЭК 19086-1:2016.

SQO «Мониторинг центров обработки данных» должен описывать процесс мониторинга в центрах обработки данных, используемых при предоставлении служб.

7.6.2.2 Безопасная утилизация и повторное использование оборудования

Описание процессов безопасной утилизации или повторного использования оборудования.

SQO «Безопасная утилизация или повторное использование оборудования» должен описывать процессы безопасной утилизации и повторного использования оборудования.

Процесс безопасной утилизации и повторного использования оборудования должен обеспечивать удаление данных на устройствах хранения, а также определять процедуру утилизации неиспользуемого

оборудования. В ИСО/МЭК 19086-1:2016 (пункт 10.12.8) содержится описание компонента SLA «Удаление данных».

7.6.2.3 Доступ на объекты

Положение о политике и процессе предоставления доступа на объекты, используемые для предоставления соответствующих служб.

SQO «Доступ на объекты» должен описывать политику и процесс предоставления доступа на объекты, используемые для предоставления служб.

7.6.3 Рекомендации

В ИСО/МЭК 27002 приводится описание мер физической безопасности и защиты от воздействий окружающей среды.

В ИСО/МЭК 27040 содержится информация о методах удаления данных с устройств хранения.

7.7 Компонент «Безопасность при эксплуатации»

7.7.1 Описание

Компонент «Безопасность при эксплуатации» определяет и документирует процессы, используемые для обеспечения безопасности в процессе эксплуатации предоставляемых служб.

Компонент «Безопасность при эксплуатации» должен определять фактически используемые процессы обеспечения безопасности в процессе эксплуатации предоставляемых служб.

7.7.2 Целевые параметры уровня обслуживания

7.7.2.1 Срок отправки отчетов об уязвимостях

Максимальный период времени, отводимый поставщику облачной службы для отправки потребителю облачной службы отчета о выявленной уязвимости.

Примечание — SQO «Процесс управления уязвимостями» описывает уязвимости, о которых создается отчет (подпункт 7.7.3.3).

SLO «Срок отправки отчетов об уязвимостях» должен определять максимальное время, отводимое поставщику облачной службы, на отправку потребителю облачной службы отчета об уязвимостях, имеющих отношение к предоставляемым службам, после их выявления.

7.7.2.2 Срок хранения журналов

Заданный срок хранения журналов, в течение которого они доступны для анализа потребителями облачной службы.

SLO «Срок хранения журналов» должен определять срок, в течение которого журналы доступны для анализа потребителями предоставляемых служб.

7.7.3 Целевые параметры качества обслуживания

7.7.3.1 Защита от вредоносного программного обеспечения

Положение, описывающее механизмы обеспечения доступности и планового использования антивирусных средств, предоставляемых поставщиком облачной службы для предоставляемых служб.

SQO «Защита от вредоносного программного обеспечения» должен описывать механизмы обеспечения доступности и планового использования средств антивирусной защиты для предоставляемых служб.

7.7.3.2 Регистрация и мониторинг

Положение, описывающее процессы регистрации и мониторинга в отношении безопасности предоставляемых служб, а также способов получения журналов и отчетов мониторинга потребителями облачных служб.

SQO «Регистрация и мониторинг» должен описывать процедуры ведения журнала и мониторинга в отношении безопасности предоставляемых служб, а также способы получения таких журналов и отчетов мониторинга потребителями облачных служб.

7.7.3.3 Управление уязвимостями

Описание процесса мониторинга, обнаружения технических уязвимостей, оповещения о них и их устранения путем установки пакетов исправлений для предоставляемых служб.

SQO «Управление уязвимостями» должен описывать процесс мониторинга, обнаружения технических уязвимостей, оповещения о них и их устранения путем установки пакетов исправлений для предоставляемых служб.

7.7.3.4 Метод оповещения об уязвимостях

Описание метода, с помощью которого поставщик уведомляет потребителя облачной службы о технических уязвимостях и их устранениях для предоставляемых служб.

SQO «Метод оповещения об уязвимостях» должен описывать метод, используемый поставщиком для уведомления потребителя облачной службы о технических уязвимостях и соответствующих исправлениях для предоставляемых служб.

7.7.3.5 Описание угрозы уязвимости

Описание процесса, используемого поставщиком облачной службы для предоставления информации об угрозах уязвимостей.

SQO «Описание угрозы уязвимости» описывает процесс, используемый поставщиком облачной службы для предоставления информации об угрозах уязвимостей для предоставляемых служб.

7.7.4 Рекомендации

В ИСО/МЭК 30111 приводится описание процесса управления уязвимостями.

В ИСО/МЭК 29147 содержится дополнительное описание процесса информирования об угрозах, связанных с уязвимостями.

Управление изменениями рассматривается в ИСО/МЭК 19086-1:2016 (см. 10.10.1).

7.8 Компонент «Безопасность коммуникаций»

7.8.1 Описание

Компонент «Безопасность коммуникаций» определяет потребности в обеспечении безопасности сети и любых других каналов связи, используемых для предоставления служб.

Компонент «Безопасность коммуникаций» должен описывать средства защиты сетей и каналов связи, используемых для предоставления служб.

7.8.2 Целевые параметры качества обслуживания

Разделение сетей

Описание технических мер и средств для разделения сетевого доступа между пользователями в многопользовательской среде, между административными функциями поставщика и средой потребителя облачной службы, а также для предотвращения несанкционированного обмена данными между пользователями.

SQO «Разделение сетей» должен описывать технические средства, с помощью которых обеспечивается разделение сетевого доступа для предоставляемых служб.

7.8.3 Рекомендации

ИСО/МЭК 27033 (все части) содержит инструкции по реализации системы безопасности связи, состоящей из механизма обеспечения сетевой безопасности, шлюзов безопасности, VPN и средств безопасности беспроводной связи.

В пункте 13.2.1 ИСО/МЭК 27002:2013 содержится дополнительная информация о безопасности системы связи.

7.9 Компонент «Приобретение, разработка и поддержка систем»

7.9.1 Описание

В компоненте «Приобретение, разработка и поддержка систем» содержится описание мер по обеспечению информационной безопасности в процессе приобретения, разработки и непрерывного обслуживания систем в отношении предоставляемых служб.

Компонент «Приобретение, разработка и поддержка систем» должен описывать меры по обеспечению информационной безопасности в процессе приобретения, разработки и обслуживания систем в отношении предоставляемых служб.

7.9.2 Целевые параметры качества обслуживания

7.9.2.1 Процедуры приобретения систем

Описание процедур, используемых CSP в отношении мер обеспечения информационной безопасности, применяемых в процессе приобретения систем или компонентов у третьих сторон с целью их использования для предоставляемых служб.

SQO «Процедуры приобретения систем» должен описывать процедуры поставщика облачной службы в отношении мер обеспечения информационной безопасности при приобретении систем или компонентов у третьих сторон с целью их использования для предоставления служб.

7.9.2.2 Процедуры безопасной разработки

Описание процедур, используемых CSP для безопасной разработки предоставляемых служб и связанных систем.

SQO «Процедуры безопасной разработки» должен описывать процедуры, используемые CSP при разработке предоставляемых служб и связанных систем.

7.9.2.3 Процедуры поддержки систем

Положение о мерах по обеспечению информационной безопасности, которые предпринимает поставщик облачной службы для обеспечения безопасной работы предоставляемых служб. В качестве примера можно привести процедуры обновления программного и аппаратного обеспечения, а также соответствующей документации.

Примечание — Управление уязвимостями рассматривается в 7.7.3.3.

SQO «Процедуры поддержки систем» должен описывать меры по обеспечению информационной безопасности, которые поставщик облачной службы предпринимает для обеспечения безопасной эксплуатации предоставляемых служб.

7.9.3 Рекомендации

Процедуры приобретения, разработки и поддержки систем описаны в ИСО/МЭК 27017. Безопасная утилизация выведенного из эксплуатации оборудования описана в ИСО/МЭК 27040.

Управление рисками рассматривается в ИСО 31000.

ИСО/МЭК 27034 (все части) предоставляет дополнительные сведения о защите приложений на протяжении всего жизненного цикла их разработки.

7.10 Компонент «Взаимоотношения с поставщиками»

7.10.1 Описание

Управление взаимоотношениями с поставщиками является неотъемлемой частью облачных служб, и компонент «Взаимоотношения с поставщиками» определяет соответствующие подходы к управлению.

Компонент «Взаимоотношения с поставщиками» должен описывать методы управления взаимоотношениями с поставщиками для предоставляемых служб.

7.10.2 Целевые параметры качества обслуживания

Управление взаимоотношениями с поставщиками

Описание реализуемых CSP процедур по приобретению, использованию, защите, мониторингу, поддержке и анализу эффективности сторонних служб.

SQO «Управление взаимоотношениями с поставщиками» должен предоставлять описание реализуемых CSP процедур по приобретению, использованию, защите, мониторингу, поддержке и анализу эффективности сторонних служб, используемых для обеспечения предоставляемых потребителю служб.

7.10.3 Рекомендации

Информация об эффективном управлении взаимоотношениями с поставщиками в процессе предоставления облачных служб приведена в ИСО/МЭК 27036-4, ИСО/МЭК 27002 и ИСО/МЭК 27017.

7.11 Компонент «Менеджмент инцидентов информационной безопасности»

7.11.1 Описание

Компонент «Менеджмент инцидентов информационной безопасности» определяет процесс и действия, которые необходимо предпринять в отношении инцидентов, возникающих в предоставляемых службах.

Компонент «Менеджмент инцидентов информационной безопасности» должен документировать процесс и действия, которые необходимо предпринять в отношении инцидентов, возникающих в предоставляемых службах.

7.11.2 Целевые параметры уровня обслуживания

Период уведомления об инцидентах информационной безопасности

Описание максимального периода времени, необходимого поставщику для уведомления потребителя облачной службы о возникновении инцидента информационной безопасности.

SLO «Период уведомления об инцидентах информационной безопасности» должен описывать максимальный период времени, необходимый поставщику для уведомления потребителя облачной службы о возникновении инцидента информационной безопасности для предоставляемых служб.

7.11.3 Целевые параметры качества обслуживания

Менеджмент инцидентов информационной безопасности

Положение, документирующее процедуры управления инцидентами информационной безопасности, используемые поставщиком облачной службы.

SQO «Менеджмент инцидентов информационной безопасности» должен документировать процедуры управления инцидентами информационной безопасности, используемые поставщиком облачной службы для предоставляемых служб.

7.11.4 Рекомендации

ИСО/МЭК 27035-1 и ИСО/МЭК 27035-2 описывают процедуры управления инцидентами информационной безопасности.

ИСО/МЭК 19086-1:2016 (см. 10.8.1) предоставляет дополнительные SLO и SQO для управления инцидентами.

7.12 Компонент «Менеджмент непрерывности деятельности организации»

7.12.1 Описание

Компонент «Менеджмент непрерывности деятельности организации» определяет процессы, используемые поставщиком облачной службы для обеспечения непрерывности бизнеса для предоставляемых служб.

Компонент «Менеджмент непрерывности деятельности организации» должен документировать процессы, используемые поставщиком облачной службы для обеспечения непрерывности бизнеса в предоставляемых службах.

7.12.2 Целевые параметры качества обслуживания

Процесс обеспечения непрерывности деятельности организации

Положение, описывающее процесс, используемый поставщиком облачной службы для обеспечения непрерывности бизнеса облачной службы.

SQO «Процесс обеспечения непрерывности деятельности организации» должен описывать процесс, используемый поставщиком облачной службы для обеспечения непрерывности бизнеса в отношении предоставляемых служб.

7.12.3 Рекомендации

ИСО/МЭК 19086-1:2016 (см. 10.11.2) описывает SLO и SQO, относящиеся к надежности и отказоустойчивости услуг. ИСО/МЭК 19086-1:2016 (см. 10.11.4) описывает SLO и SQO, относящиеся к аварийному восстановлению.

ИСО/МЭК 27031:2011 (см. 6.7) описывает процедуры измерения производительности ИКТ для определения готовности ИКТ.

ИСО/МЭК 27031:2011 (см. 8.4.2) описывает процедуры качественной и количественной оценки производительности ИКТ для определения готовности ИКТ.

7.13 Компонент «Соответствие нормативным требованиям»

7.13.1 Описание

На клиента облачной службы могут быть наложены обязательства в отношении соответствия определенным стандартам, политикам и правилам в области безопасности при использовании предоставляемых служб. Компонент «Соответствие нормативным требованиям» описывает методы, которые поставщик облачной службы может использовать для демонстрации такого соответствия.

Компонент «Соответствие нормативным требованиям» должен описывать аспекты соответствия нормативным требованиям, по которым поставщик облачной службы аттестован, в отношении предоставляемых служб.

7.13.2 Целевые параметры качества обслуживания

Примечание — ИСО/МЭК 19086-1:2016 (см. 10.13) предоставляет SQO для аттестаций, сертификаций и аудитов, которые поставщик облачной службы может использовать, чтобы продемонстрировать соответствие стандартам, политикам и правилам в целом. Указанные SQO могут применяться, в частности, для демонстрации соответствия конкретным стандартам, политикам и правилам обеспечения безопасности.

7.13.3 Рекомендации

ИСО 19600 описывает системы управления соответствием нормативным требованиям.

8 Защита персональных данных

8.1 Компонент «Согласие и возможность выбора»

8.1.1 Описание

Поставщик должен предоставить потребителю облачной службы средства, позволяющие владельцам ПДн выбирать и выражать свое согласие в отношении обработки их ПДн.

Компонент «Согласие и возможность выбора» должен описывать возможности выбора и выражения согласия владельцами ПДн в предоставляемых службах.

Примечание — Основные принципы защиты ПДн описаны в ИСО/МЭК 29100.

8.1.2 Целевые параметры качества обслуживания

Возможности для выражения согласия владельцами ПДн

Описание механизмов, реализованных в предоставляемых службах и позволяющих владельцам ПДн выбирать и выражать свое согласие в отношении обработки их ПДн.

SQO «Возможности для выражения согласия владельцами ПДн» должен содержать описание механизмов, реализованных в предоставляемых службах и позволяющих владельцам ПДн выбирать и выражать свое согласие в отношении обработки их ПДн.

8.1.3 Рекомендации

Рекомендации описаны в ИСО/МЭК 27018:2014 (приложение А.1).

8.2 Компонент «Законность и декларация целей обработки персональных данных»

8.2.1 Описание

Компонент «Законность и декларация целей обработки персональных данных» описывает целевые параметры качества обслуживания, определяющие законность обработки ПДн потребителя облачной службы, включая любые обязательства ограничить обработку ПДн рамками, заданными в CSA.

Компонент «Законность и декларация целей обработки персональных данных» должен формировать основу для законной обработки ПДн в предоставляемых службах.

8.2.2 Целевые параметры качества обслуживания

8.2.2.1 Законность целей обработки персональных данных

Утверждение о том, что поставщик облачной службы обрабатывает ПДн только для целей, явно указанных в соглашении об облачной службе.

Утверждение о том, что поставщик облачной службы обрабатывает ПДн в соответствии с соответствующими юридическими, нормативными и договорными обязательствами.

SQO «Законность целей обработки персональных данных» должен декларировать, что ПДн обрабатываются только для целей, указанных в CSA для предоставляемых служб, и что такая обработка осуществляется в соответствии с соответствующими юридическими, нормативными и договорными обязательствами.

8.2.2.2 Список доступа третьих лиц

Список третьих лиц, согласованный поставщиком и потребителем облачной службы, исключая указанных в списке, подготовленном в соответствии с 8.6.2.1 (список субподрядчиков по обработке ПДн), которые имеют доступ к ПДн, имеющим отношение к потребителю облачной службы, включая пользователей и клиентов потребителя облачной службы.

SQO «Список доступа третьих лиц» должен перечислить третьи стороны (кроме субподрядчиков), имеющие доступ к ПДн, имеющим отношение к потребителю облачной службы, для предоставляемых служб.

8.2.3 Рекомендации

ИСО/МЭК 19944 содержит описание категорий данных, используемых в облачных службах, а также рекомендации по созданию заявлений об использовании данных, включающих необходимые требования. Заявления об использовании данных, подготовленные в соответствии с ИСО/МЭК 19944, могут использоваться поставщиком облачной службы для определения конкретного использования данных в предоставляемых службах и подготовки заявлений об ограничении их законного использовании и сбора.

Рекомендации также описаны в ИСО/МЭК 27018:2014 (приложение А.2).

8.3 Компонент «Минимизация данных»

8.3.1 Описание

Компонент «Минимизация данных» задает требования к минимизации обработки и доступа к ПДн. Такая минимизация может быть достигнута путем ограничения максимального времени хранения временных файлов, сокращения числа заинтересованных сторон, имеющих доступ к ПДн, или минимизации генерации и раскрытия ПДн техническими (криптографическими) средствами в самой облачной службе.

Компонент «Минимизация данных» должен описывать требования к минимизации обработки и доступа к ПДн в предоставляемых службах.

8.3.2 Параметры уровня обслуживания

Максимальное время хранения временных файлов

Максимальный период, в течение которого временные файлы, созданные в процессе обработки, будут храниться, прежде чем они будут удалены или станут окончательно недоступны.

SLO «Максимальное время хранения временных файлов» должен определять максимальный период, в течение которого временные файлы, содержащие ПДн, сгенерированные во время обработки, хранятся предоставляемыми службами.

8.3.3 Целевые параметры качества обслуживания

8.3.3.1 Минимизация доступа заинтересованных сторон

Положение, описывающее политику минимизации количества лиц, которым раскрываются ПДн или которые имеют доступ к ПДн, а также объем такого доступа.

SQO «Минимизация доступа заинтересованных сторон» должен описывать политику минимизации количества лиц, которым раскрываются ПДн или которые имеют доступ к ПДн для предоставляемых служб.

8.3.3.2 Криптографические средства для минимизации объема и доступа к персональным данным

Описание криптографических средств, доступных для минимизации объема и доступа к ПДн, обрабатываемых предоставляемыми службами.

SQO «Криптографические средства для минимизации объема и доступа к персональным данным» должен предоставлять описание криптографических средств, доступных для минимизации объема и доступа к ПДн, обрабатываемых предоставляемыми службами.

8.3.4 Рекомендации

Рекомендации описаны в ИСО/МЭК 27018:2014 (приложение А.4).

Дополнительные сведения приведены в ИСО/МЭК 19086-1:2016 (см. 10.12.8).

В ИСО/МЭК 29100:2011 (см. 2.23) рассматриваются методы обработки. ИСО/МЭК 29100:2011 (см. 5.5) дает определение минимизации данных.

8.4 Компонент «Ограничение использования, хранения и раскрытия»

8.4.1 Описание

Компонент «Ограничение использования, хранения и раскрытия» должен описывать ограничения, связанные с использованием, хранением и раскрытием ПДн в предоставляемых службах.

8.4.2 Целевые параметры качества обслуживания

Заявления об использовании данных

Заявления поставщика облачной службы о том, как он использовал данные, которые могут потенциально содержать ПДн.

SQO «Заявления об использовании данных» должен описывать, как поставщик облачной службы использовал все данные, которые могут потенциально содержать ПДн, в предоставляемых службах.

8.4.3 Рекомендации

Вопросы хранения данных рассматриваются в ИСО/МЭК 19086-1:2016 (см. 10.7.1.1).

Раскрытие ПДн в соответствии с требованиями правоохранительных/регулирующих органов описано в ИСО/МЭК 19086-1:2016 (см. 10.12.11.3).

Элементы управления и соответствующие рекомендации по внедрению приведены в ИСО/МЭК 27018:2014 (приложение А.5).

Вопросы ограничения использования, хранения и раскрытия ПДн рассмотрены в ИСО/МЭК 27018:2014 (приложение А.5).

Заявления об использовании данных и используемые классификации данных описаны в ИСО/МЭК 19944.

8.5 Компонент «Точность и качество»

8.5.1 Описание

Компонент «Точность и качество» описывает целевые параметры качества обслуживания, связанные с точностью, целостностью и качеством ПДн.

Компонент «Точность и качество» должен описывать средства, с помощью которых предоставляемые службы обеспечивают точность, полноту, актуальность и адекватность обрабатываемых ПДн с точки зрения цели их использования.

8.5.2 Целевые параметры качества обслуживания

Целостность, точность и качество персональных данных

Положение, описывающее политику и процесс, используемые для проверки целостности, точности и качества собираемых, хранимых и обновляемых ПДн.

SQO «Целостность, точность и качество персональных данных» должен описывать политику и процесс, используемые для проверки целостности, точности и качества собираемых, хранимых и обновляемых ПДн в предоставляемых службах.

8.5.3 Рекомендации

Рекомендации описаны в ИСО/МЭК 27018:2014 (приложение А.6).

Рекомендации в отношении точности и качества ПДн даны в ИСО/МЭК 29100.

8.6 Компонент «Открытость, прозрачность и наблюдаемость»

8.6.1 Описание

Компонент «Открытость, прозрачность и наблюдаемость» описывает SQO, относящиеся к субподрядчикам из числа привлекаемых поставщиком облачной службы, имеющим доступ к ПДн, и механизмы, которые поставщик облачной службы использует для получения и сохранения согласий на сбор, обработку и сохранение ПДн.

Компонент «Открытость, прозрачность и наблюдаемость» должен описывать процесс уведомления о сборе и обработке ПДн, а также любых субподрядчиках, привлекаемых для обработки ПДн, в предоставляемых службах.

8.6.2 Целевые параметры качества обслуживания

8.6.2.1 Список субподрядчиков, обрабатывающих персональные данные

Список субподрядчиков поставщика облачной службы, которые имеют доступ к данным потребителя облачной службы, содержащим ПДн.

SQO «Список субподрядчиков, обрабатывающих персональные данные» должен содержать список субподрядчиков, привлекаемых для обработки ПДн в предоставляемых службах.

8.6.2.2 Требование явного согласия

Если поставщик облачной службы собирает ПДн, необходимо подготовить описание средств, посредством которых поставщик облачной службы направляет уведомление владельцам ПДн о сборе,

обработке и сохранении ПДн, а также описание средств, посредством которых поставщик облачной службы получает и сохраняет их согласия.

SQO «Требование явного согласия» должен описывать средства, посредством которых поставщик облачной службы направляет уведомление владельцам ПДн о сборе, обработке и сохранении ПДн, а также средства, посредством которых поставщик облачной службы получает и сохраняет их согласия в предоставляемых службах в случае, если поставщик облачной службы собирает ПДн.

8.6.3 Рекомендации

Рекомендации также описаны в ИСО/МЭК 27018:2014 (приложение А.7).

В тех случаях, когда для обработки ПДн не требуется согласие владельца (например, когда обработка ПДн осуществляется в соответствии с требованиями законодательства), SQO «Требование явного согласия» не будет детально описывать получение и сохранение согласий владельцев ПДн.

8.7 Компонент «Индивидуальное участие и доступ»

8.7.1 Описание

Компонент «Индивидуальное участие и доступ» описывает средства, позволяющие владельцам ПДн получать и просматривать свои ПДн, ставить под сомнение точность и полноту ПДн, вносить дополнения и исправления или удалять ПДн в зависимости от ситуации и доступных возможностей в конкретном контексте.

Компонент «Индивидуальное участие и доступ» должен описывать средства, с помощью которых владельцы ПДн могут получать доступ, просматривать, дополнять, исправлять и удалять свои ПДн в предоставляемых службах.

8.7.2 Целевые параметры качества обслуживания

8.7.2.1 Участие и доступ субъекта персональных данных

Если поставщик облачной службы собирает ПДн, необходимо подготовить положение, описывающее механизмы, посредством которых поставщик облачной службы поддерживает процессы обработки и реагирования на жалобы, опасения или вопросы от владельцев ПДн в отношении методов и средств защиты, применяемых поставщиком облачной службы при работе с ПДн, в том числе полученных непосредственно и через потребителя облачной службы.

SQO «Участие и доступ субъекта персональных данных» должен описывать механизмы, посредством которых владельцы ПДн могут подавать жалобы, описывать проблемы или задавать вопросы поставщику облачной службы и получать ответы в отношении предоставляемых служб.

8.7.2.2 Возможности доступа владельцев персональных данных

Компонент «Возможности доступа владельцев ПДн» описывает функции, реализованные для того, чтобы помочь владельцам ПДн воспользоваться своими правами на доступ, исправление и удаление ПДн в предоставляемых службах.

SQO «Возможности доступа владельцев ПДн» должен описывать функции, реализованные для того, чтобы помочь владельцам ПДн воспользоваться своими правами на доступ, исправление и удаление ПДн в предоставляемых службах.

8.7.3 Рекомендации

Рекомендации даны в ИСО/МЭК 29100.

8.8 Компонент «Подотчетность»

8.8.1 Описание

Компонент «Подотчетность» охватывает вопросы, связанные с гарантиями защиты ПДн. В частности, он включает в себя определение политики поставщика облачной службы в отношении уведомления потребителя облачной службы об утечках ПДн, в том числе четкое описание объема разглашенных ПДн.

Компонент «Подотчетность» должен описывать политику уведомления об утечках ПДн и политику удаления ПДн в предоставляемых службах.

8.8.2 Целевые параметры уровня обслуживания

Период уведомления об утечках ПДн

Описание максимального периода времени, необходимого поставщику облачной службы для уведомления потребителя облачной службы об утечках ПДн.

Примечание — Процесс уведомления о нарушениях в ходе обработки ПДн описан в 8.8.3.1.

SLO «Период уведомления об утечках ПДн» описывает максимальный период времени, необходимый поставщику облачной службы для уведомления потребителя облачной службы об утечках ПДн в предоставляемых службах.

8.8.3 Целевые параметры качества обслуживания

8.8.3.1 Уведомление об утечке данных

Заявление о процессе уведомления потребителя облачной службы об утечке данных и о политике, которую поставщик облачной службы применяет в случае утечки ПДн, включая в себя все процедуры и методы, применяемые для информирования об инцидентах и их устранении.

SQO «Уведомление об утечке данных» должен описывать процесс, используемый для уведомления потребителя облачной службы об утечке ПДн в предоставляемых службах.

8.8.3.2 Политика удаления ПДн

Описание политики, которую поставщик облачной службы применяет для возврата, передачи и удаления ПДн, содержащихся в облачной службе, включая любые процедуры, используемые для обеспечения недоступности таких данных.

SQO «Политика удаления ПДн» должен описывать политику, которую поставщик облачной службы применяет для возврата, передачи и удаления ПДн в предоставляемых службах.

8.8.4 Рекомендации

Рекомендации также описаны в ИСО/МЭК 27018:2014 (приложение А.9).

Вопросы удаления данных в случае прекращения оказания услуг описаны в ИСО/МЭК 19086-1:2016 (см. 10.7.1.2 и 10.12.8).

8.9 Компонент соответствия условий обработки персональных данных законодательству

8.9.1 Описание

Компонент соответствия условий обработки ПДн законодательству предназначен для определения стран/юрисдикций, в которых предоставляемые службы могут хранить ПДн.

Компонент соответствия условий обработки ПДн законодательству (в конкретном SLA) должен определять страны/юрисдикции, в которых ПДн хранятся предоставляемыми службами.

8.9.2 Целевые параметры качества обслуживания

Места обработки и хранения ПДн

Список географических местоположений, где ПДн хранятся и обрабатываются. Местоположение должно включать в себя сведения о юрисдикции, включая страну, а также более детальные сведения, такие как город.

SQO «Места обработки и хранения ПДн должен определять сведения о географических местоположениях, где предоставляемые службы хранят и обрабатывают ПДн.

8.9.3 Рекомендации

Рекомендации приведены в ИСО/МЭК 19086-1:2016 (см. 10.12.9).

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального, межгосударственного стандарта
ISO/IEC 17788:2014	IDT	ГОСТ ISO/IEC 17788—2016 «Информационные технологии. Облачные вычисления. Общие положения и терминология»
ISO/IEC 19086-1	IDT	ГОСТ Р ИСО/МЭК 19086-1—2019 «Информационные технологии. Облачные вычисления. Структура соглашения об уровне обслуживания (SLA). Часть 1. Обзор и концепции»
ISO/IEC 27017	—	*
ISO/IEC 27018	—	*
ISO/IEC 29100	IDT	ГОСТ Р ИСО/МЭК 29100—2013 «Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности»

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

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:
- IDT — идентичные стандарты.

Библиография

[1] ISO/IEC 17789, Information technology — Cloud computing — Reference architecture

[2] ISO/IEC 19086-2, Information technology — Cloud computing — Service level agreement (SLA) framework — Part 2: Metric Model

[3] ISO/IEC 19086-3, Information technology — Cloud computing — Service level agreement (SLA) framework — Part 3: Core conformance requirements

[4] ISO 19600, Compliance management systems — Guidelines

[5] ISO/IEC 19944, Information technology — Cloud computing — Cloud services and devices: Data flow, data categories and data use

[6] ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

[7] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

[8] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls

[9] ISO/IEC 27031, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

[10] ISO/IEC 27033, Information technology — Security techniques — Network security — Part 1: Overview and concepts

[11] ISO/IEC 27035-1, Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management

[12] ISO/IEC 27035-2, Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response

[13] ISO/IEC 27036-4, Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services

[14] ISO/IEC 27040, Information technology — Security techniques — Storage security

[15] ISO/IEC 29147, Information technology — Security techniques — Vulnerability disclosure

[16] ISO/IEC 30111, Information technology — Security techniques — Vulnerability handling processes

[17] ISO 31000, Risk management — Principles and guidelines

[18] ITU-T Recommendation Y.3502, Information technology — Cloud computing — Reference architecture

[19] ITU-T Recommendation Y.3500, Information technology — Cloud computing — Overview and vocabulary

[20] ISO/IEC JTC 1/SC 27, WG 5 Standing Document 2 — Part 1: Privacy References List. Последняя версия доступна по адресу http://www.jtc1sc27.din.de/sbe/wg5SD2-1

УДК 006.34:004:006.354 ОКС 35.210

Ключевые слова: Соглашение об уровне обслуживания (SLA), поставщик облачной службы (CSP), потребитель облачной службы (CSC), компоненты обеспечения информационной безопасности, персональные данные (ПДн)

БЗ 12—2020

Редактор *П.К. Одинцов*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 11.11.2020. Подписано в печать 01.12.2020. Формат 60 × 84 $^{1}/_{8}$. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,24.
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