ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 70288— 2022

Информационные технологии

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ

Руководство по формированию политики

(ISO/IEC TR 22678:2019, NEQ)

Издание официальное

Москва
Российский институт стандартизации
2022

Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО «ИАВЦ»), Институтом системного программирования им. В.П. Иванникова РАН (ИСП РАН)

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 17 августа 2022 г. № 779-ст.

4 Настоящий стандарт разработан с учетом основных нормативных положений международного документа ISO/IEC TR 22678:2019 «Информационные технологии. Облачные вычисления. Руководство по формированию политики» (ISO/IEC TR 22678:2019 «Information technology — Cloud computing — Guidance for policy development», NEQ)

5 ВВЕДЕН ВПЕРВЫЕ

6 Федеральное агентство по техническому регулированию и метрологии не несет ответственности за патентную чистоту настоящего стандарта

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.rst.gov.ru)

Содержание

Введение

В настоящее время облачные вычисления стремительно развиваются и включают в себя глобальную сеть больших и малых центров обработки данных и телекоммуникационных сетей, управляемых множеством разных поставщиков облачных служб, предлагающих своим клиентам большое количество различных облачных служб. Предлагаемые облачные сервисы варьируются от простых приложений для работы с электронной почтой или повышения производительности, заменяющих традиционное локальное программное обеспечение, до расширенных сервисов, которые невозможно создать каким-либо другим способом, таких как сервисы социальных сетей, обработка больших данных, машинное обучение и когнитивные сервисы.

Облачные вычисления предлагают множество преимуществ клиентам облачных служб, государствам и обществу.

Как и в случаях других коммерческих услуг, государство и организации принимают политики, направленные на обеспечение защиты интересов клиентов и государства.

Как отмечено в Соглашении ВТО о технических барьерах в торговле, стандарты играют жизненно важную роль в поддержке технических регламентов и оценке соответствия, однако настоящий стандарт не распространяется на вопросы торговли.

Настоящий стандарт содержит информацию, которая поможет в разработке политик размещения и использования облачных вычислительных систем и служб.

Настоящий стандарт необходимо применять с учетом требований нормативных правовых актов и стандартов Российской Федерации, в том числе и в области персональных данных и защиты информации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ

Руководство по формированию политики

Information technology.
Cloud computing.
Guidance for policy development

Дата введения — 2023—03—30

1 Область применения

В настоящем стандарте представлены рекомендации по использованию национальных и межгосударственных стандартов в качестве инструмента при разработке политик, определяющих или регулирующих поставщиков облачных служб и облачные службы, а также политик и методов, регулирующих использование облачных служб в организациях.

Настоящий стандарт включает в себя материалы, объясняющие концепции облачных вычислений и роль национальных и межгосударственных стандартов облачных вычислений в формировании политик и методов.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты.

ГОСТ ISO/IEC 17788—2016 Информационные технологии. Облачные вычисления. Общие положения и терминология

ГОСТ ISO/IEC 29100 Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных

ГОСТ Р ИСО/МЭК 17826 Информационные технологии. Интерфейс управления облачными данными (CDMI)

ГОСТ Р ИСО/МЭК 19086-1 Информационные технологии. Облачные вычисления. Структура соглашения об уровне обслуживания (SLA). Часть 1. Обзор и концепции

ГОСТ Р ИСО/МЭК 19086-4 Информационные технологии. Облачные вычисления. Структура соглашения об уровне обслуживания (SLA). Часть 4. Компоненты информационной безопасности и защиты персональных данных

ГОСТ Р ИСО/МЭК 19941 Информационные технологии. Облачные вычисления. Интероперабельность и переносимость

ГОСТ Р ИСО/МЭК 27001 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

ГОСТ Р ИСО/МЭК 27002 Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности

ГОСТ Р ИСО/МЭК 27017 Информационные технологии. Методы и средства обеспечения безопасности. Правила применения мер обеспечения информационной безопасности на основе ИСО/МЭК 27002 при использовании облачных служб

Издание официальное

ГОСТ Р ИСО/МЭК 27018 Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки

ГОСТ Р ИСО/МЭК 27036-4 Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 4. Рекомендации по обеспечению безопасности облачных услуг

ГОСТ Р ИСО/МЭК 27050-1 Информационные технологии. Методы обеспечения безопасности. Выявление и раскрытие электронной информации. Часть 1. Обзор и концепции

ГОСТ Р ИСО/МЭК 30134-2 Информационные технологии. Центры обработки данных. Ключевые показатели эффективности. Часть 2. Коэффициент энергоэффективности (PUE)

ГОСТ Р ИСО/МЭК 38500 Информационные технологии. Стратегическое управление ИТ в организации

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.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ ISO/IEC 17788, а также следующие термины с соответствующими определениями:

3.1 **облачные вычисления** (cloud computing): Парадигма для предоставления возможности сетевого доступа к масштабируемому и эластичному пулу общих физических или виртуальных ресурсов с предоставлением самообслуживания и администрированием по требованию.

Примечание — Примеры ресурсов включают серверы, операционные системы, сети, программное обеспечение, приложения и оборудование для хранения данных.

3.2 **юрисдикция** (jurisdiction): Географическая или корпоративная область, на которую распространяется политика облачных вычислений.

Примечание — В контексте государственной политики это, как правило, географический район, над которым орган, принимающий политику, имеет законные полномочия либо в качестве правительства, либо в качестве уполномоченного регулирующего органа. Однако в среде предприятия или государственного учреждения юрисдикция политики может охватывать бизнес-функцию, отдел, агентство или другую организационную область ответственности, не связанную с географией.

3.3

оператор данных (data operator): Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами осуществляющие обработку персональных данных.

[Адаптировано из [1], статья 3]

3.4 **обработчик данных** (data processor): Лицо, которое обрабатывает данные по поручению оператора.

Примечание — Оператор данных определяет цели обработки данных, а обработчик обрабатывает данные исключительно согласно инструкциям оператора.

4 Сокращения

В настоящем стандарте применены следующие сокращения.

ВТО — Всемирная торговая организация;
ИКТ — информационно-коммуникационные технологии;
ИТ — информационные технологии;
ПДн — персональные данные;
ПК — персональный компьютер;
СМИБ — система менеджмента информационной безопасности;
DDoS — распределенный отказ в обслуживании (атака) (distributed denial of service);
IaaS — инфраструктура как услуга (infrastructure as a service);
PaaS — платформа как услуга (platform as a service);
SaaS — программное обеспечение как услуга (software as a service);
SLA — соглашение об уровне обслуживания (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).

5 Содержание настоящего стандарта

5.1 Цель настоящего стандарта

Цель настоящего стандарта — облегчение разработки, основанной на стандартах, государственных и корпоративных политик, способствующих внедрению и использованию услуг облачных вычислений.

Следуя рекомендациям, приведенным в настоящем стандарте, разработчики политики могут:

- надлежащим образом использовать национальные и межгосударственные стандарты при разработке политик;
- добиться большей согласованности применимых законов, правил и политик;
- снизить затраты поставщиков и потребителей облачных служб;
- увеличить выбор и повысить конкуренцию;
- упростить развертывание и внедрение экономичных локальных или глобальных облачных служб.

5.2 Целевая аудитория

Настоящий стандарт предназначен:

а) для представителей законодательной власти всех уровней;

б) органов, уполномоченных в области обеспечения безопасности и защиты информации;

в) разработчиков корпоративных политик, включая:

1) потребителей облачных служб (крупных и мелких) и потенциальных потребителей;
2) поставщиков облачных служб;
3) партнеров по облачным службам;

г) разработчиков негосударственных правил и политик доверия и прозрачности облачных вычислений в торговых организациях и инженерных учреждениях;

д) организаций, оказывающих консультативные услуги государству и предприятиям по экономическим и политическим последствиям развития технологической политики.

5.3 Применение настоящего стандарта

В настоящем стандарте приведены рекомендации по применению конкретных национальных и межгосударственных стандартов при разработке политик в области облачных вычислений, а также рекомендации о том, как эти стандарты лучше использовать с учетом [1] и [2].

6 Аспекты облачных вычислений, влияющие на разработку политики

6.1 Общие положения

В данном разделе рассмотрены ключевые характеристики и понятия облачных вычислений, понимание которых необходимо разработчикам государственной или корпоративной политики для облачных служб. Цель раздела — предоставить материал в легкочитаемой и доступной форме для тех, кто не является профессионалом в области облачных вычислений, и предоставить ссылки на доступные дополнительные технические материалы, которые могут потребоваться.

6.2 Основные характеристики облачных вычислений

6.2.1 Стандартное определение облачных вычислений

Определение облачных вычислений (см. 3.1) отражает несколько существенных характеристик облачных вычислений, отличных от характеристик традиционных, локальных вычислений или вычислений на сервере (см. также ГОСТ ISO/IEC 17788 и [3]). В приложении А приведены ключевые характеристики облачных вычислений, их описание и выводы.

Определение говорит о том, что облачные вычисления включают в себя предоставление практически любых ресурсов ИКТ в виде услуги по сети (облачной услуги) и что такое предоставление может выполняться динамически по требованию потребителя облачных служб, во многом аналогично тому, как предоставляются другие, например телекоммуникационные, услуги. Клиенты используют то, что им нужно, когда им это нужно, а потребление услуг оплачивается соответственно. Включение и отключение услуги предоставления доступа к ИКТ ресурсу может быть таким же простым, как включение и отключение света с помощью выключателя. Необходимые длительные процессы приобретения, установки, настройки, защиты и эксплуатации оборудования, программного обеспечения и приложений потребителем облачных служб значительно сокращаются, если не исключаются полностью.

6.2.2 Основные характеристики облачных вычислений (ГОСТ ISO/IEC 17788)

Основные характеристики облачных вычислений приведены в таблице 1.

Таблица 1 — Основные характеристики облачных вычислений

Характеристика	Особенность облачных вычислений
Широкий сетевой доступ	Облачная служба может быть доступна из произвольного места с помощью разных типов устройств, включая ПК и мобильные устройства всех типов, подключенных разными способами, как правило, через сеть Интернет, но иногда и через частные сети, такие как внутренняя корпоративная сеть
Измеримое обслуживание	Использование клиентами облачной службы учитывается, и с них может взиматься плата в зависимости от того, что они действительно использовали, подобно тому как оплачивается электроэнергия на основе измеренного количества потребленной энергии. Таким образом, сокращение использования может означать снижение затрат
Многопользовательский доступ	Многопользовательский доступ означает, что ресурсы, предоставляемые облачной службой, совместно используются несколькими потребителями облачных служб. Использование ресурсов каждым отдельным пользователем изолировано и недоступно для всех остальных пользователей таким образом, что потребители облачных служб могут быть уверены в том, что их данные и работа с приложениями невидимы для всех других потребителей, т. е. реквизиты банковского счета не будут видны другим клиентам банка. Следует отметить, что один потребитель может иметь несколько различных пользователей данной облачной службы, например в случае, если деятельность различных отделов организации должна быть изолирована одна от другой. Кроме того, следует обратить внимание на то, что хотя у частного облака по определению только один потребитель облачных служб, этот единственный потребитель может иметь несколько собственных изолированных пользователей
Самообслуживание по требованию	Как правило, облачные службы позволяют клиенту регистрироваться, оплачивать и использовать службу без необходимости взаимодействия с представителем службы поддержки клиентов. Кроме того, как правило, клиенты могут управлять своей услугой или отменять ее без вмешательства кого-либо. Могут возникать исключительные обстоятельства, когда требуется взаимодействие с человеком-оператором, но это происходит в нестандартных случаях, а не в обычной деловой практике

Окончание таблицы 1

Характеристика	Особенность облачных вычислений
Оперативная гибкость и масштабируемость	Облачные службы способны динамически распределять ресурсы для конкретной рабочей нагрузки по мере необходимости. В таких случаях зачастую говорят о вертикальном масштабировании (увеличении размера одного ресурса) или о горизонтальном масштабировании (выделении дополнительных аналогичных ресурсов). Цель масштабирования заключается в том, чтобы клиенты могли увеличивать или сокращать использование облачной службы как можно более динамично, как правило, для того, чтобы справиться с запланированным или неожиданным увеличением или уменьшением рабочей нагрузки. Например, если вебсайт, размещенный в облаке, неожиданно стал вызывать большой интерес, то владелец сайта может заказать (и заплатить) больше вычислительной мощности и пропускной способности, чтобы избежать перегруженности сайта. Как только пик пройден, ресурсы могут быть высвобождены, а стоимость снижена. Еще одним важным аспектом масштабируемости облачных служб является то, что объем доступных ресурсов кажется клиенту практически неограниченным в отличие от традиционных центров обработки данных, где количество серверов, объем хранилища данных, пропускная способность сети, как правило, ограничены и могут быть изменены только путем установки дополнительного оборудования
Пул ресурсов	Облачные вычисления повышают эффективность за счет разделения различных ресурсов между несколькими пользователями и рабочими нагрузками. Например, в традиционных вычислениях возможна ситуация, когда 10 клиентов используют 10 отдельных серверов, даже если каждый из них использует только половину мощности каждого сервера. В среде облачных вычислений такие 10 клиентов могут быть автоматически распределены для использования не более пяти серверов

6.3 Основные преимущества облачных вычислений

6.3.1 Преимущества для потребителей облачных служб

Преимущества для потребителей облачных служб приведены в таблице 2.

Таблица 2 — Преимущества для потребителей облачных служб

Характеристика	Особенность облачных вычислений
Низкие капиталовложения	Заказчику, желающему разработать или запустить новое приложение, больше не требуется собственное оборудование ИТ, а также здания и инфраструктура, необходимые для его размещения и поддержки. Кроме того, потенциально нет необходимости приобретать, устанавливать и эксплуатировать большую часть приложений. Клиент может заплатить относительно небольшую сумму (нет необходимости покупать серверное оборудование) за разработку и/или развертывание нового приложения, а затем постепенно наращивать объем ресурсов облачного сервера, которые он использует, по мере увеличения использования приложения и доходов
Рентабельность облачного масштабирования	Поставщики облачных служб имеют возможность покупать ресурсы в требуемом масштабе, а это значит, что если серверы и другие ресурсы приобретаются в больших количествах, то они обходятся намного дешевле. Подобная экономия затрат может сказываться и на отдельных клиентах. Кроме того, стоимость работы одного сервера в больших центрах обработки данных, с точки зрения рабочей силы, энергии и других затрат, намного ниже, чем суммарно в сотнях небольших центров
Использование по мере необходимости	Облачные службы позволяют клиентам начинать с малого, а затем очень быстро подниматься и опускаться по мере необходимости. Клиент может уменьшить свои счета в спокойные для своего бизнеса периоды и увеличить мощности по мере возрастания или в ответ на пиковые нагрузки, связанные, например, с сезонными распродажами или неожиданной популярностью
Конкуренция	Из-за динамики рынка цены на облачные службы основаны на конкуренции. У каждого нового проекта есть выбор, какого поставщика облачных служб использовать, а новые стартапы в этой области продолжают бросать вызов крупным операторам с особыми функциями и инновациями

Окончание таблицы 2

Характеристика	Особенность облачных вычислений
Безопасность	В свое время для перехода на использование облачных служб безопасность считалась вопросом, требующим пристального внимания, но сегодня безопасность больше не считается серьезным препятствием для внедрения облачных вычислений. На это есть несколько причин. Во-первых, у поставщиков облачных служб, имеющих высокую репутацию, как правило, есть группы безопасности, работающие круглосуточно для того, чтобы обеспечить безопасность своих систем, своевременно устанавливать исправления безопасности и опережать любые возникающие угрозы, которые могут быть идентифицированы. Они очень быстро реагируют на инциденты. Даже крупным коммерческим предприятиям будет сложно нанять и оплатить эквивалентный уровень экспертных знаний в области безопасности в формате 24 × 7 для своих собственных сотрудников. Во-вторых, одной из самых серьезных угроз компьютерной безопасности является «внутренняя» атака, когда к нарушению причастен кто-то с административным или физическим доступом, возможно, коррумпированный или недовольный сотрудник, но у которого нет такого же доступа к внешним облачным службам (см. [4])
Доступность и надежность	Многие поставщики облачных служб управляют несколькими центрами обработки данных в разных местах, и это дает клиентам возможность повысить доступность своих приложений и данных. Приложения можно запускать в нескольких центрах обработки данных, а данные могут быть распределены между этими центрами обработки данных, что позволяет избежать единой точки отказа. Если один центр обработки данных отключается из-за стихийного бедствия или крупного сбоя, доступ потребителей облачных служб к приложениям и данным может быть мгновенно переключен на другой центр обработки данных
Расширенные возможности	Все чаще происходит так, что поставщики облачных служб обеспечивают доступность расширенных возможностей в виде готовых облачных служб. Примерами таких возможностей являются системы искусственного интеллекта, расширенная аналитика и службы больших данных. Некоторые из этих служб предварительно обучены на обширных наборах данных. Потребителю облачных служб может быть трудно реализовать подобные расширенные возможности своими силами из-за ограниченного доступа к квалифицированному персоналу и ресурсам. Зачастую гораздо выгоднее интегрировать передовые облачные службы в новые приложения потребителя облачных служб
Выбор модели развертывания облачных служб	Облачные вычисления позволяют потребителю облачных служб выбрать наиболее подходящую для удовлетворения своих требований модель развертывания из числа публичных, частных, общественных и гибридных моделей развертывания облачных служб (см. ГОСТ ISO/IEC 17788). Для модели развертывания частного облака поставщик облачных служб будет частью собственной организации потребителя облачных служб
Более простое соблюдение требований	Большинство поставщиков общедоступных облачных служб получают различные сертификаты для своих облачных служб. Используя возможности этих облачных служб, потребитель облачных служб снимает с себя большую часть бремени получения сертификатов и обеспечения соответствия. Кроме того, поставщики облачных служб часто предоставляют консультации, рекомендации и поддержку своим потребителям облачных служб, которые стремятся к тому, чтобы использование ими облачных служб соответствовало требованиям конфиденциальности и правилам защиты данных в их юрисдикции

6.3.2 Преимущества облачных вычислений для общества

Преимущества облачных вычислений для общества в целом представлены в таблице 3.

Таблица 3 — Преимущества облачных вычислений для общества

Преимущества для общества	С точки зрения облачных вычислений
Энергоэффективность	Большие специально построенные центры обработки данных могут быть гораздо более энергоэффективными, чем большинство более мелких. Они также могут располагаться в местах с дешевой электроэнергией или там, где используемая энергия получается из возобновляемых источников энергии. Некоторые центры обработки данных спроектированы даже для эксплуатации с воздушным охлаждением, что значительно снижает потребность в энергии. Кроме того, поставщики облачных служб могут оптимизировать рабочие нагрузки своих клиентов и данные для работы на минимально необходимом количестве серверов[1)]
Надежность и устойчивость	Подключения к облачным службам надежно защищены и гораздо менее уязвимы для атак вирусов и вредоносных программ. Они также часто достаточно устойчивы, чтобы противостоять отдельным распределенным атакам типа «отказ в обслуживании» (DDoS) со стороны хакеров и ботов. Поставщики облачных служб часто предлагают географическое разнообразие, так что облачные службы могут продолжаться в случае крупного стихийного бедствия, отключившего один из их центров обработки данных. Кроме того, поскольку эти системы, как правило, используют программное обеспечение для обеспечения устойчивости совокупности нескольких физических машин, то не требуется надежная работа каждого компьютера. Поэтому в большом центре обработки данных облачных служб нет необходимости тщательно отслеживать состояние каждого сервера. С большой вероятностью рабочие нагрузки могут быть перемещены без ущерба для клиента. Служба остается устойчивой даже при отказе отдельных серверов. Вышедшее из строя оборудование может быть восстановлено и использовано повторно или переработано в зависимости от обстоятельств. Устойчивость облачных служб приносит ощутимую пользу обществу, поскольку потребители облачных служб больше не зависят от собственных ресурсов и навыков для обеспечения функционирования бизнес-процессов
Законный доступ	Хотя конфиденциальность клиентов важна, общество также должно защищать себя от злоумышленников. При хранении данных в облачных службах, а не на локальных компьютерах, существуют дополнительные процедуры получения должным образом санкционированного законного доступа к этим данным для расследований уголовных преступлений, для борьбы с терроризмом и других государственных целей. Однако в данном случае отсутствует универсальный подход, поскольку имеются как юридические, так и инженерные проблемы. Смежной областью является раскрытие электронной информации во время судебных разбирательств (см. ГОСТ Р ИСО/МЭК 27050-1)

[1)] Малый бизнес, переходящий в облако, может существенно снизить потребление энергии и выбросы углерода за счет запуска своих бизнес-приложений в облаке вместо запуска тех же приложений в собственной инфраструктуре.

6.4 Рекомендации для разработчиков политик

6.4.1 Совместная ответственность

В связи со спецификой облачных вычислений, когда потребители и пользователи облачных служб обладают значительным контролем над использованием облачных служб, они разделяют обязанности по обеспечению безопасности, приватности, конфиденциальности и целостности служб.

Например, при использовании облачных служб потребители облачных служб несут ответственность за применение передовых методов для обработки паролей или других учетных данных, для предоставления соответствующих разрешений конкретным пользователям, для представления типов данных, которые они помещают в облачную службу, и для надлежащей маркировки контента, чтобы облачная служба могла его правильно обработать. Такие методы определяют общую безопасность, приватность, конфиденциальность и целостность служб, но не подконтрольны исключительно поставщику облачных служб.

Широкое признание получило использование определенных отраслевых норм и правил для руководства как поставщиками, так и потребителями облачных служб при эксплуатации и использовании облачных служб.

6.4.2 Облачные сервисы в нескольких юрисдикциях

Традиционно ИТ-системы развертывались внутри организации или в среде размещения внутри отдельной страны или юрисдикции. Международная телекоммуникационная инфраструктура строилась от страны к стране с четкими точками присоединения, определенными на международных границах, так что ресурсы и средства управления, используемые персоналом, располагались в той же юрисдикции, что и клиенты службы. Для большинства систем и служб облачных вычислений это не актуально.

Глобальные облачные службы достигают масштабируемости и эффективности за счет максимально возможной централизации своей деятельности, управления и персонала. Это означает, что клиенты в одном месте могут использовать ресурсы облачных служб, такие как, например, серверы, хранилища данных и сетевое оборудование, расположенные в другом месте, а управление этими серверами осуществляется из третьего места.

Такой подход дает много следующих преимуществ как поставщику облачных служб, так и их потребителям:

- наличие единой глобальной версии пакета программного обеспечения для облачной службы означает, что одна группа разработки, тестирования и безопасности может поддерживать всю сеть центров обработки данных поставщика облачных служб, независимо от их количества и стран, в которых они расположены;
- как поставщики облачных служб, так и потребители получают выгоду от постоянных и своевременных улучшений служб, и нет необходимости индивидуального внедрения обновлений;
- обновления и исправления безопасности разворачиваются легко. Уязвимости или нарушения, выявленные в разных местах, могут быть устранены одновременно везде;
- использование географически разнообразного размещения и предоставления услуг и данных может обеспечить резервирование и защиту от серьезных инцидентов, таких как наводнение, землетрясение или отказ сети, которые могут вывести из строя весь центр обработки данных. Содержание нескольких центров обработки данных в некоторых регионах может оказаться нерентабельным или неэффективным, поэтому резервирование за пределами региона может быть единственным вариантом для удовлетворения требований непрерывности бизнеса;
- для данных, которые не ограничены географически, облачная служба может динамически перемещать или копировать данные между центрами обработки данных для оптимизации производительности и использования хранилища. Например, некоторые данные могут быть актуальны для чтения во всем мире, возможно, на мобильных устройствах (например, карты, новости, видео), так что глобальная репликация значительно улучшает качество обслуживания клиентов за счет уменьшения задержки доступа к данным. Такое перемещение и репликация данных, как правило, полностью автоматизированы на основе объективных оценок поведения при использовании данных.

6.4.3 Экономика управления глобальной облачной службой

Устойчивость и гибкость поставщиков облачных служб, особенно крупных организаций, позволяют минимизировать стоимость их капитальных вложений и эксплуатационных расходов и, возможно, снизить цены на предложения своих облачных служб. Поставщики облачных служб, как правило, используют стандартные конфигурации оборудования в своих центрах обработки данных, что позволяет им приобретать оборудование в больших объемах. Серверы, используемые в облачных центрах обработки данных, как правило, не обеспечивают многих дополнительных и несущественных функций, которые характерны для типовых серверов, что экономит затраты и энергию. Чтобы обеспечить непрерывность бизнеса, поставщики облачных служб повышают отказоустойчивость в основном за счет программного обеспечения, а не за счет резервирования оборудования, что еще больше снижает капитальные и эксплуатационные расходы. Таким образом, для крупного центра обработки данных облачных служб основная задача заключается не в том, чтобы поддерживать все оборудование в рабочем состоянии, а в том, чтобы распределять рабочие нагрузки таким образом, чтобы потребитель облачных служб не замечал ни аппаратных сбоев, ни изменений в службах. Подобная отказоустойчивость может потребовать использования определенных стилей архитектуры программного обеспечения или шаблонов проектирования для приложений, специально разработанных для облаков с тем, чтобы сделать сбои незаметными для пользователей облачных служб.

Благодаря масштабности крупных облачных центров обработки данных поставщиков облачных служб такие центры проектируются для минимального энергопотребления с тем, чтобы снизить затраты и максимизировать плотность вычислений, чего невозможно достичь в небольших центрах обработки данных. Облачные серверы не нуждаются в таких интерфейсах, как, например, мониторы, мыши и клавиатуры, и они не используются в конструкциях серверов, монтируемых в стойку. Кроме того,

поставщики облачных служб заинтересованы в разработке высокоэффективных систем охлаждения и распределения энергии, снижающих воздействие на окружающую среду. Поставщики облачных служб инициируют индивидуальные проекты в области возобновляемых источников энергии для питания своих центров обработки данных, и они могут использовать передовые, экологически чистые источники энергии, такие как топливные элементы, работающие на биомассе. В зависимости от местоположения помимо использования возобновляемых источников энергии рециркуляция генерируемого тепла может использоваться, например, для отопления местных жилых помещений. Методики и оценка энергоэффективных центров обработки данных рассматриваются в [5] и [6].

Использование одной версии программного обеспечения во всех центрах обработки данных — это еще один способ снижения затрат поставщиками услуг связи. Поставщик облачных служб будет стремиться использовать одно и то же программное обеспечение для каждой службы во всей своей сети центров обработки данных. Соответственно это программное обеспечение может контролироваться, управляться и обслуживаться одной командой (включая аналитиков безопасности). Новые версии программного обеспечения будут тестироваться и выпускаться постепенно, чтобы снизить риск возникновения катастрофической ошибки во всей сети, но цель останется — иметь, насколько это возможно, единую развернутую версию программного обеспечения во всех службах поставщика облачных служб.

Если существует несколько версий программного обеспечения, то каждое изменение необходимо будет протестировать на всех активных версиях, а каждую уязвимость безопасности необходимо будет проверять и исправлять во всех версиях. Таким образом, стоимость обслуживания увеличивается примерно пропорционально квадрату количества используемых версий.

Согласованность аппаратного и программного обеспечения также позволяет автоматизировать управление облачными службами. Для обнаружения потенциальных сбоев и аномалий поставщики облачных служб могут использовать различные способы мониторинга миллионов серверов и процессов. Применение, например, искусственного интеллекта повышает непрерывность бизнеса и снижает затраты как поставщика облачных служб, так и их потребителей.

6.4.4 Возможности глобальных масштабируемых общедоступных облачных вычислений

Общедоступные облачные службы с высокой степенью масштабируемости, развернутые глобально, предлагают экономичные и масштабируемые услуги вне зависимости от географического положения. Такие службы предлагают возможности, которые не были доступны в традиционных локальных системах или частных облаках. Такие глобальные службы позволяют собирать и передавать между различными локациями пользовательские данные, а также организационные данные. Объем и скорость сбора и передачи данных беспрецедентны.

Благодаря внедрению методов анализа данных и машинного обучения с использованием возможностей общедоступных облачных служб и больших объемов собранных данных более чем когда-либо необходимо понимать происхождение и категории данных. Кроме того, для защиты отдельных лиц, а также для защиты конфиденциальной информации организации по мере агрегирования и обезличивания данных (см. [1] и [7]) разработчики политик государственного и корпоративного уровня должны понимать необходимые концепции, терминологию и инструменты информирования о желаемом поведении и результатах.

6.4.5 Влияние масштабирования и скорости обслуживания

Ключевой характеристикой облачных вычислений является то, что эта услуга является «самообслуживанием по требованию» (см. ГОСТ ISO/IEC 17788—2016, подраздел 6.2). Это означает, что клиенты могут создать учетную запись, оплатить выбранную услугу, начать ее использовать, публиковать контент, вносить изменения или делать что-то еще, что облачная служба предоставляет для них посредством высокоавтоматизированного процесса. Высокая скорость работы служб высоко ценится потребителями облачных служб и является основной движущей силой внедрения облачных служб. Однако поставщику облачных служб сложно выделить нарушителя со стороны потребителя облачной службы по его поведению. Примерами нарушений являются использование облачной службы в злонамеренных целях, например распространение вредоносных программ, совместное использование незаконного или экстремального контента, нарушение авторских прав, неосторожное использование, такое как размещение конфиденциальной информации в незащищенных местах или неосведомленное использование, например размещение неприемлемого или незаконного контента.

Хотя поставщики облачных служб постоянно работают над устранением последствий действий нарушителей, авторизованные или не авторизованные нарушители со стороны пользователя облачной службы постоянно совершенствуют свои навыки и инструменты. Для предотвращения последствий не-

надлежащего использования своих услуг поставщики облачных служб используют как специалистов, так и средства искусственного интеллекта.

При необходимости ответственность и управление контролем доступа и использования среды возлагаются на потребителей облачных служб. Например, потребителю облачных служб необходимо контролировать авторизацию и аутентификацию в своих облачных службах, чтобы гарантировать, что их пользователи не будут злоупотреблять облачными службами. Кроме того, потребитель облачных служб должен отслеживать контент и использование своих облачных служб, чтобы гарантировать соблюдение всех применимых местных, национальных и международных законов (см. 6.4.1).

6.4.6 Влияние постоянного развития

До появления облачных вычислений программное обеспечение выпускалось в виде крупных «релизов», часто с разницей в два или более года. Такой подход позволял проводить большое количество испытаний и сертификаций перед реализацией каждого релиза. На практике обновление от одной версии к другой часто требовало отключения систем, обновления с новым кодом и повторного запуска либо сразу, либо на группах машин, что приводило к запланированному перерыву для обслуживания. В случае сбоя обновления необходимо было выполнить обратный процесс. Кроме того, обновлениям безопасности зачастую приходилось ждать недели или месяцы для развертывания «пакета обновления» или другой возможности обновления программного обеспечения.

Облачные вычисления из-за своего круглосуточного режима работы и современной среды угроз безопасности перешли к модели непрерывного развития, при которой небольшие инкрементальные изменения вносятся очень часто, как правило еженедельно или ежедневно. Исправления безопасности при необходимости могут быть развернуты незамедлительно.

В результате больше не существует четкого графика выпуска реализаций с длительными периодами тщательно запланированных процессов тестирования или сертификации. В облачной системе традиционный цикл утверждения для устаревшей системы не будет завершен до того, пока она не будет переведена на новую версию с дальнейшими изменениями уже в процессе. Следовательно, процессы тестирования и сертификации должны адаптироваться к среде постоянных изменений программного обеспечения. Еще одним результатом будет то, что тестирование может быть более целенаправленным. Вероятно, что некоторые ошибки не будут выявлены собственными проверками поставщика услуг и повлияют на клиентов. Однако в равной степени верно и то, что исправление проблем может быть реализовано гораздо быстрее.

6.4.7 Влияние совместного использования облачных служб

Поскольку облачные ресурсы, такие как компьютеры, хранилище и сети, представляют собой объединенные ресурсы, совместно используемые многими потребителями и/или пользователями облачных служб (см. 6.2.2), то становится невозможным предоставление коммерческим аудиторам или государственным инспекторам физического доступа к оборудованию, используемому одним потребителем облачных служб, без потенциального нарушения конфиденциальности других потребителей облачных служб, использующих тот же ресурс. Некоторые данные могут быть распределены по нескольким общим ресурсам хранения с использованием «сегментирования».

В каждом случае потребитель облачных служб контролирует свои собственные данные, а поставщик облачных служб может не иметь возможности просматривать или контролировать отдельные данные в облачном хранилище данных клиента, если они, например, зашифрованы.

Это также означает, что полностью безопасное удаление данных, которое в соответствии с некоторыми старыми политиками может потребовать уничтожения носителя, не может выполняться так же часто или быстро, как в системах с одним клиентом. Если данные одного клиента занимают только 10 % места на жестком диске, то неэкономично и неэффективно запрещать его использование другими клиентами до тех пор, пока диск не будет окончательно выведен из эксплуатации.

Многоуровневый подход к безопасному удалению, не требующий уничтожения носителя, приведен в [7, подпункт 9.2.8.5].

Когда дело доходит до расследования в рамках закона, физический доступ к ресурсам, совместно используемым большим количеством пользователей удаленно, не подходит. В данном случае требуется облачно-ориентированный подход, основанный на возможностях облачных сервисов для поддержки запросов и удаления. Во многих случаях данные облачных журналов на уровне приложения могут предоставлять сведения о доступе к сеансу и действиях для обеспечения аудита, ведения журналов и расследований.

6.4.8 Влияние географических ограничений

У крупных глобальных поставщиков облачных служб могут быть разные подходы к хранению статических данных. Когда клиент решает хранить (или генерировать) данные, поставщик облачных служб должен принимать взвешенные решения о том, где они будут храниться.

Соображения, которые необходимо учитывать при принятии такого решения поставщиком, включают в себя:

- клиентские или юридические требования или политики;
- текущую доступную емкость хранилища (например, для очень больших объемов);
- производительность хранилища (ближайший центр обработки данных может быть сильно загружен из-за других клиентов, что замедляет доступ к данным и снижает пропускную способность, а более удаленный центр обработки данных загружен существенно менее);
- затраты на хранение (хранение в одних местах может стоить поставщику облачных служб больше, чем в других, например, из-за разницы в стоимости энергии или других эксплуатационных расходов);
- пропускную способность и доступность сети (иногда подключение к удаленному узлу лучше, чем к локальному);
- потребители облачных служб могут быть вынуждены подчиняться политикам и правилам обеспечения непрерывности бизнеса (аварийного восстановления), которые требуют от них поддержки географически разделенных копий своих данных. В некоторых случаях может оказаться невозможным обеспечение резервного хранилища в пределах одного географического расположения. Кроме того, как правило, требуется, чтобы избыточные ресурсы были размещены на расстоянии, достаточном для предотвращения выхода из строя как основного, так и резервного ресурса в результате крупномасштабных стихийных бедствий и техногенных катастроф;
- у многих потребителей облачных служб есть полевой персонал, клиенты, поставщики и/или партнеры, расположенные в других регионах. Локальное хранение данных, необходимых этим пользователям, может повысить производительность служб;
- потребители облачных служб могут собирать и обрабатывать данные локально и объединять свои локальные данные в более крупном объекте в другой юрисдикции. Такой подход используется либо из-за проблем с задержкой в сети, либо с целью сокращения объема данных, которые необходимо передать в головной центр обработки данных (например, данные из тысяч мобильных приложений, от устройств Интернета вещей или из других источников сбора данных);
- географические ограничения данных не всегда предотвращают их утечку из местоположения с ограниченным доступом, поскольку большинство уязвимостей систем безопасности используются удаленно. Внутренние ресурсы и неправильная настройка данных вручную также могут быть причиной потери данных, но их влияние может быть смягчено в более эффективной глобальной облачной среде.

Некоторые политики, как государственные, так и корпоративные, могут требовать, чтобы некоторые или все данные, хранящиеся в облачной службе, физически хранились в пределах определенной юрисдикции. В частности, при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации (см. [1]).

Географически ограниченное хранение данных может оказаться более дорогостоящим из-за накладных расходов на управление, меньшей эффективности хранения, а также может привести к снижению производительности приложений из-за сетевых задержек или недостаточной пропускной способности.

В небольших юрисдикциях может оказаться очень мало поставщиков облачных служб с локальным центром обработки данных. Даже если такой есть, может оказаться невозможным только с одним центром обработки данных обеспечить географическое резервирование в соответствующей юрисдикции, в результате чего повышается уязвимость к любым локальным катастрофам (см. 6.4.12).

6.4.9 Необходимость категоризации и классификации данных облачных служб

Облачные службы содержат большие объемы данных, принадлежащих как поставщику облачных служб, так и их клиентам. Чтобы оптимизировать использование и управление данными, их следует категорировать; в ГОСТ ISO/IEC 17788 приведены три основные категории облачных данных, а [7] дополняет эти категории до четырех категорий данных верхнего уровня, а также предоставляет подробную таксономию для множества различных подкатегорий.

Имеются следующие четыре категории верхнего уровня:

- данные клиента облачной службы, которые предоставляются или генерируются самим потребителем облачных служб, например документы, базы данных, проекты, списки клиентов, записи персонала и т. д.;
- данные поставщика облачных служб, которые касаются операций облачной службы и не имеют отношения к потребителю облачных служб, например конфигурации оборудования, сетевые маршруты, записи об обслуживании, списки сотрудников поставщика облачных служб и т. д.;
- данные, производные от облачной службы, которые возникают в результате использования клиентом облачной службы, например, записи о его действиях, журналы вызовов, журналы аудита и т. д;
- данные учетной записи, например контактная информация и платежная информация потребителя облачных служб.

В каждой облачной службе будут присутствовать все эти категории, и все они потенциально могут содержать некоторые ПДн, подлежащие защите в соответствии с [1] и [2].

Подход, основанный на политике, которая применяет соответствующие правила к конкретным, ограниченным и четко определенным категориям данных, например перечисленным в [4], обеспечивает гораздо более эффективное управление данными, а следовательно, повышает экономическую эффективность облачной службы. В результате задача аудита соответствия становится более ясной.

Применение соответствующих ограничений к данным, которые действительно содержат ПДн, гораздо более рентабельно и эффективно для оператора данных, чем применение контроля к широкому спектру категорий данных, которые потенциально могут содержать ПДн, поскольку, как отмечалось выше, объем последних намного больше.

Обработчик данных, как правило, не знает, содержат ли те или иные данные какую-либо персональную информацию.

Обработка данных, содержащих ПДн, должна отвечать требованиям федеральных законов [1] и [2].

При обработке данных, не содержащих ПДн, необходимо использовать существенно разные подходы для надлежащей обработки текущей, конфиденциальной или ценной информации и устаревших, общедоступных или бесполезных данных.

Ответственность потребителей и пользователей облачных служб за обеспечение безопасности облачных служб для защиты общественного сектора и контроля рабочих нагрузок описана в 6.4.1.

6.4.10 Совместимость и переносимость

6.4.10.1 Общие положения

Совместимость (функциональная совместимость) — это способность двух или более связанных систем обмениваться информацией и использовать ее совместно. Например, ПК и принтер совместимы, если ПК может отправлять документ на принтер для печати, а принтер может понять формат и содержание документа.

Переносимость бывает двух видов:

- переносимость данных — это когда объекты данных (например, документы, изображения, файлы или базы данных) могут быть скопированы или перемещены из одной системы в другую, после чего могут использоваться во второй системе;
- переносимость приложений — это когда исполняемое программное обеспечение может быть скопировано или перемещено из одной системы в другую, и его можно использовать (запускать) во второй системе.

Функциональная совместимость и переносимость подробно рассматриваются в ГОСТ Р ИСО/МЭК 19941.

6.4.10.2 Вопросы взаимодействия в среде облачных вычислений

ГОСТ ISO/IEC 17788—2016, пункт 3.1.5, определяет функциональную совместимость как способность двух или более систем или приложений обмениваться информацией и совместно использовать такую информацию. Далее, в контексте облачных вычислений, функциональная совместимость рассматривается как сквозная функциональность, обеспечивающая системам потребителя облачных служб возможность взаимодействовать с облачной службой и обмениваться информацией в соответствии с предписанным методом и получать предсказуемые результаты (см. ГОСТ ISO/IEC 17788—2016, подраздел 6.6). Функциональная совместимость также включает в себя способность одной облачной службы взаимодействовать с другими облачными службами (см. [8, пункт 8.5.5] и ГОСТ Р ИСО/МЭК 19941).

На вопрос о возможности или невозможности функциональной совместимости и переносимости облачных вычислений редко можно ответить однозначно. Зачастую возможность функциональной со-

вместимости зависит от затрат на внедрение. Чтобы понять, оправданны ли ресурсы, необходимые для обеспечения обмена информацией в предписанном методе при получении предсказуемых результатов, требуется проанализировать соотношение затрат к выгодам. Способность систем потребителя облачных служб и облачных служб, а также нескольких облачных служб взаимодействовать — это нечто большее, чем способность обмена через интерфейс между системами, а следовательно, и более дорогостоящее. Кроме того, любые изменения, вызванные требованиями к взаимодействию, могут повлечь за собой необходимость в дополнительном обучении конечных пользователей, управленческого и операционного персонала.

При оценке возможностей взаимодействия с облаком необходимо рассматривать множество факторов:

- способность потребителя облачных служб взаимодействовать с облачной службой путем обмена информацией в соответствии с предписанным методом с получением предсказуемых результатов;
- возможность облачной службы работать с другими облачными службами;
- характеристики, необходимые для обеспечения успешного взаимодействия между средствами ИКТ организации и облачными службами;
- роли и действия (см. [8]);
- типы возможностей облачных вычислений, определенные в ГОСТ ISO/IEC 17788;
- интерфейсы между различными функциональными компонентами (см. [8, подраздел 9.2]).

6.4.10.3 Соображения по переносимости в среде облачных вычислений

В контексте облачных вычислений переносимость относится к способности потребителя облачных служб перемещать и соответствующим образом адаптировать свои приложения и данные между системами потребителя облачных служб и облачными службами, между различными моделями развертывания облачных вычислений и между облачными службами разных поставщиков облачных служб. В ГОСТ Р ИСО/МЭК 19941 отдельно рассмотрены переносимость облачных приложений и переносимость облачных данных.

Переносимость может напрямую зависеть от затрат на переключения. Для определения целесообразности переносимости приложений и/или данных требуется оценка затрат и выгод. Таким образом, схожесть систем потребителя облачных служб и поставщика облачных служб в большей степени заключается в снижении стоимости переключения, чем в обеспечении переносимости, поскольку переносимость возможна практически в любом случае, если заказчик желает и может за нее платить. Проблемы переключения не ограничиваются затратами; это, как правило, связано с некоторыми рисками и требует затрат времени и усилий потребителя облачных служб и, возможно, периода перерыва в обслуживании.

При рассмотрении переносимости облачных вычислений необходимо учитывать множество факторов, например:

- предоставление возможности потребителям облачных служб переносить приложения и данные в соответствии с потребностями бизнеса, такими как более быстрое обслуживание, более низкая стоимость, большая надежность или возможность аварийного восстановления;
- более широкую доступность приложений и данных, позволяющих выйти на более широкий рынок;
- время и усилия, необходимые для переноса как приложений, так и данных, однако такие накладные расходы возможно уменьшить с помощью использования языков программирования, стандартов, инструментов, структур, моделей, вычислительных модулей и API-интерфейсов;
- ограничение ситуаций блокировки, когда потребитель облачных служб привязан к облачным службам одного поставщика облачных служб.

Поставщики облачных служб стремятся обеспечить некоторую степень взаимодействия и переносимости между своими продуктами и продуктами своих конкурентов. Это отвечает их собственным коммерческим интересам и позволяет привлечь потенциальных клиентов. Однако не допускается недооценивать технические проблемы.

6.4.11 Доверие и прозрачность

Поставщики облачных служб пришли к выводу, что для коммерческого успеха необходимо доверие потребителей и регулирующих органов к их облачным службам. Одним из определений «доверенной облачной службы» является следующее:

Доверенная облачная служба — облачная служба, которая удовлетворяет требованиям прозрачности руководства, управления и безопасности в достаточной мере для того, чтобы потребитель облачных служб не сомневался в использовании облачной службы (см. [9]).

Примечания

1 Набор требований может варьироваться в зависимости от потребителя облачной службы, характеристик облачной службы и регулирующей юрисдикции.

2 Набор требований также может быть связан с дополнительными аспектами, такими как производительность, отказоустойчивость, обратимость, SLA и т. д.

3 Прозрачность означает, что поставщик облачных служб должен обеспечить потребителя облачных служб надлежащими четкими механизмами контроля и отчетности для руководства, управления и безопасности, такими как положения SLA, онлайн-объявления, политика обработки данных и т. д.

Доверие к облачной службе подразумевает следующее:

- прозрачность. В целях обеспечения доверия поставщик облачных служб должен не только делать все правильно, но и демонстрировать это потребителям облачных служб. Это касается соблюдения соответствующих стандартов, правил и политик, часто проверяемых сертификацией, и аудитов (см. 6.4.13). Сюда же относится и предоставление потребителям и регулирующим органам официальных и не официальных отчетов в стандартных отраслевых форматах с использованием стандартизованных терминов (например, см. ГОСТ ISO/IEC 17788, ГОСТ Р ИСО/МЭК 19086-1, ГОСТ Р ИСО/МЭК 19086-4, ГОСТ Р ИСО/МЭК 27017, ГОСТ Р ИСО/МЭК 27018, [7], [10], [11]);

- безопасность. Поставщики облачных служб должны обеспечивать соответствующий уровень безопасности предлагаемых услуг. Бесплатная облачная онлайн-игра не требует высокого уровня безопасности, но для любого приложения, обрабатывающего персональные данные, а также важную конфиденциальную информацию, такую как финансовая или медицинская информация, требования безопасности будут значительно выше;

- менеджмент. Система менеджмента облачной службы должна быть способна обрабатывать требования потребителей облачных служб и различные обязательства поставщика облачных служб по соблюдению различных требований. Например, не допускается доверять облачной службе, которая является безопасной, но не может распределить данные клиентов для хранения должным образом;

- управление на уровне организации. Облачная служба с отличной безопасностью и эффективным управлением заслуживает доверия ровно настолько, насколько надежна система его корпоративного управления. Например, не может заслуживать должного доверия поставщик облачных служб, в которых генеральный директор может вносить изменения в политику обработки данных по своему усмотрению, чтобы реализовать новую бизнес-возможность, например продажу данных. Вопрос прозрачности управления может быть решен путем сертификации соответствия стандартам в этой области, таким как ГОСТ Р ИСО/МЭК 38500.

Все эти аспекты в значительной степени зависят от конкретных условий, и практически невозможно создать единый набор критериев или правил для всех.

6.4.12 Исключительные обстоятельства

Некоторые поставщики облачных служб обладают большими возможностями и ресурсами для обеспечения устойчивости и выживания при крупномасштабных стихийных бедствиях, таких как землетрясения или наводнения, которые могут повредить один или несколько центров обработки данных или изолировать их от сети. Однако, когда в пределах юрисдикции имеется только один такой объект, было бы уместно рассмотреть возможные последствия случая, если бы он подвергся серьезному выходу из строя по естественным причинам или человеческим факторам.

Если политика требует, чтобы облачная служба ограничивала некоторые данные или приложения местной юрисдикцией (см. 6.4.8), может быть целесообразным рассмотреть поправку на исключительные обстоятельства.

Организации, разрабатывающей политику, необходимо оценивать в каждом случае, лучше ли соблюдать географические ограничения, тем самым рискуя непрерывностью бизнеса, или для поставщика облачных служб допустимо продолжать предоставлять услуги из центра обработки данных в другой юрисдикции до тех пор, пока нормальное обслуживание не будет возобновлено. Это решение не допускается принимать после аварии, поскольку поставщику облачных служб необходимо подготовиться к таким изменениям заранее, до того, как первоначальный центр обработки данных будет потерян или изолирован. Например, поставщик облачных служб может предложить механизм хранения зашифрованных резервных копий данных в другой юрисдикции, чтобы их можно было расшифровать и использовать только в таких исключительных обстоятельствах.

Облачное соглашение об уровне обслуживания, предназначенное для потребителей облачных служб и поставщика облачных служб, должно определять критерии действий в исключительных обстоятельствах.

6.4.13 Соответствие, сертификация, аудит

Независимая сертификация поставщика облачных служб или потребителя облачных служб должна производиться в соответствии со стандартами на информационные технологии (см. раздел 2). Эти стандарты содержат четкие критерии, по которым аудитор может проводить оценку.

Чтобы избежать повторного проведения аудита в соответствии с новыми требованиями сертификации, рекомендуется использовать уже признанные аккредитации. Повторное использование работы, уже выполненной аккредитованным оценщиком, способствует глобальному согласованному подходу.

Поставщик облачных служб, который получает сертификацию в соответствии со стандартами, может утверждать, что его службы были оценены и проверены независимыми профессионалами, соответствуют общепризнанным стандартизованным передовым методам и им можно доверять.

После выдачи сертификата соответствия соответствующему стандарту соответствие требованиям обеспечивается внутренними процессами и периодическими внешними аудитами.

6.4.14 Проблемы внедрения на малых и средних предприятиях

6.4.14.1 Общие положения

В общем случае малые и средние предприятия, использующие облачные службы, подразделяются на две категории:

- малые и средние предприятия, не связанные с ИТ;
- ИТ-ориентированные малые и средние предприятия.

Внедрение облачных вычислительных служб на предприятиях обеих категорий имеет как преимущества, так и недостатки.

6.4.14.2 Малые и средние предприятия, не связанные с ИТ

В эту категорию входят малые и средние предприятия, для которых ИТ-услуги не связаны непосредственно с их реальным бизнесом, такие, например, как розничные торговцы, мелкие производители, фермы, товарищества, индивидуальные предприниматели и т. д. Такой тип малых и средних предприятий выберет облачные приложения, которые настроены (или могут быть настроены) на их собственные бизнес-потребности, такие как общие офисные приложения для повышения производительности — текстовые процессоры, электронные таблицы, хранилище документов, бухгалтерский учет, отслеживание запасов, телефония и т. д. Кроме того, они могут использовать специализированные приложения, разработанные для их конкретной отрасли, возможно, созданные их партнером по облачным услугам (см. ГОСТ ISO/IEC 17788).

Для малых и средних предприятий облачные вычисления значительно снижают, если не исключают совсем, необходимость иметь, управлять и защищать дополнительное программное обеспечение, отличное от установленного на их собственных настольных компьютерах или других устройствах. Им не нужно следить за работой или защитой сервера или о них беспокоиться.

Ключевым вопросом зачастую является обеспечение экономичного и надежного сетевого подключения к поставщику облачных служб с достаточной пропускной способностью. Эта проблема особенно актуальна в сельских районах, поскольку там, возможно, присутствует только один поставщик сетевых служб с невысоким стимулом развития своих услуг или вообще без него. В этом отношении малые и средние предприятия могут столкнуться с особыми трудностями. Опубликованные карты, показывающие доступность широкополосной связи, иногда вводят в заблуждение, поскольку они могут показывать покрытие сотовой связью, такой как 3G и 4G. Однако сотовая связь часто не подходит или слишком дорого обходится малым и средним предприятиям для непрерывного ежедневного использования облачных служб. Использование точек доступа Wi-Fi целесообразно для сотрудников малого и среднего бизнеса, находящихся в дороге, в том случае, если они хорошо спроектированы или хорошо обслуживаются.

Кроме того, в вопросах безопасности малые и средние предприятия пытаются соблюдать правила защиты данных и конфиденциальности, но не могут позволить себе услуги высокооплачиваемых консультантов или специалистов-профессионалов, испытывают трудности и с безопасностью. Вместо этого они должны в основном полагаться на советы и функции, предоставляемые их поставщиком облачных служб, которые зачастую могут быть непростыми для понимания в случаях, когда речь идет о соблюдении местных законов и правил. Однако облачные службы могут оказаться лучшим вариантом, чем эквивалентное локальное программное обеспечение, поскольку высока вероятность того, что поставщик облачных служб имеет больший опыт и навыки для обеспечения соответствия по сравнению с организацией малого и среднего бизнеса.

6.4.14.3 Малые и средние предприятия, ориентированные на ИТ

В эту категорию входят малые и средние предприятия, такие как ориентированные на ИТ стартапы, которые сразу выбирают облачные вычисления в качестве платформы развития своего нового бизнеса. Они могут воспользоваться преимуществами начала работы с минимальными капиталовложениями, а затем в зависимости от своих рыночных возможностей расти медленно или быстро.

Успешный малый и средний бизнес такого рода может быстро завоевать облачных клиентов по всему миру и обеспечить источник существенных экспортных доходов для своей родной юрисдикции. Некоторые из этих малых и средних предприятий могут превратиться в центры инноваций и доходов и даже стать влиятельными во всем деловом мире.

Поскольку такие малые и средние предприятия, как правило, находятся в городах, то имеют лучший доступ к широкополосной сети (сети Интернет), чем первая группа. Однако они могут столкнуться с трудностями понимания и прогнозирования того, как их новая бизнес-модель воспринимается контролирующими (надзорными) органами, особенно в случаях, если их подход может нарушать принятые деловые и социальные нормы.

6.4.14.4 Влияние политики крупного бизнеса на малые и средние предприятия

Обе категории предприятий малого и среднего бизнеса могут быть несоразмерно затронуты политикой, направленной в первую очередь на регулирование крупных предприятий.

Например, новый регламент может требовать привлечения юриста и подрядчика по обработке данных для крупного предприятия с численностью в 10 000 сотрудников, а также требовать таких же юриста и подрядчика для начинающего бизнеса с пятью сотрудниками, что может выйти за рамки финансирования малого и среднего бизнеса или сделать невозможным их внедрение облачных вычислений.

Любое несоразмерное воздействие на малые и средние предприятия может иметь серьезные экономические последствия там, где малые и средние предприятия составляют значительную часть местного делового сообщества. В то время как крупные поставщики облачных служб гораздо меньше затронуты непосредственно, потеря местного бизнеса малых и средних предприятий может негативно повлиять также и на крупных поставщиков облачных служб, тем самым снижая общую ценность всей местной облачной экосистемы и лишая местных жителей некоторых из указанных выше преимуществ.

7 Использование национальных и межгосударственных стандартов при разработке политики облачных вычислений

7.1 Национальные и межгосударственные стандарты, относящиеся к разработке политики облачных вычислений

В таблице 4 приведено краткое описание стандартов облачных вычислений.

Таблица 4 — Стандарты облачных вычислений

Стандарт облачных вычислений	Описание
ГОСТ ISO/IEC 17788	Содержит обзор облачных вычислений, а также набор терминов и определений. Предоставляет терминологическую основу для стандартов облачных вычислений
[8]	Задает эталонную архитектуру облачных вычислений. Эталонная архитектура включает в себя роли облачных вычислений, действия облачных вычислений, а также функциональные компоненты облачных вычислений и их взаимосвязи
ГОСТ Р ИСО/МЭК 17826	Определяет интерфейс управления облачными данными (CDMI)
ГОСТ Р ИСО/МЭК 19086-1	Определяет набор общих блоков облачных SLA (концепций, терминов, определений, контекстов), которые могут быть использованы для создания Соглашений об уровне обслуживания (SLA)
[10]	Устанавливает общую терминологию, определяет модель для определения метрик для соглашений об уровне облачных вычислений (SLA) и включает приложения модели с примерами

Окончание таблицы 4

Стандарт облачных вычислений	Описание
[11]	Определяет основные требования соответствия для соглашений об уровне обслуживания (SLA) для облачных служб на основе ГОСТ Р ИСО/МЭК 19086-1 и руководства по основным требованиям соответствия. Предназначен для использования как поставщиками облачных служб, так и потребителями облачных служб
ГОСТ Р ИСО/МЭК 19086-4	Определяет безопасность и защиту компонентов персональных данных, SLO и SQO для соглашений об уровне обслуживания облачных вычислений (SLA для облачных вычислений), включая требования и рекомендации
ГОСТ Р ИСО/МЭК 19941	Определяет типы взаимодействия и переносимости облачных вычислений, взаимосвязь и взаимодействие между этими двумя аспектами облачных вычислений, а также общую терминологию и концепции, используемые для обсуждения совместимости и переносимости, особенно в отношении облачных служб
[3]	Содержит обзор облачных вычислений, а также набор терминов и определений
[12]	Технический отчет, описывающий основные технологии и методы облачных вычислений
[7]	Определяет и описывает категории данных, потоки данных между устройством и поддерживающими облачными службами, а также способы описания использования различных категорий данных поставщиком облачных служб
ГОСТ Р ИСО/МЭК 27001	Определяет требования для создания, внедрения, поддержки и постоянного улучшения системы менеджмента информационной безопасности в контексте организации. Также включает в себя требования к оценке и обработке рисков информационной безопасности с учетом потребностей организации. Требования, изложенные в ГОСТ Р ИСО/МЭК 27001, являются общими и предназначены для применения ко всем организациям, независимо от их типа, размера или характера
ГОСТ Р ИСО/МЭК 27002	Дает рекомендации по стандартам информационной безопасности организации и методам управления информационной безопасностью, включая выбор, внедрение и управление средствами контроля, принимая во внимание среду(среды) риска информационной безопасности организации
ГОСТ Р ИСО/МЭК 27017	Дает рекомендации по мерам обеспечения информационной безопасности, применимым к предоставлению и использованию облачных служб, обеспечивая: - дополнительное руководство по внедрению соответствующих мер обеспечения безопасности, приведенных в ГОСТ Р ИСО/МЭК 27002; - дополнительные меры обеспечения безопасности с руководством по внедрению, которые конкретно относятся к облачным службам
ГОСТ Р ИСО/МЭК 27018	Устанавливает общепринятые цели, меры обеспечения безопасности и руководящие принципы для реализации мер по защите персональных данных (ПДн) в соответствии с принципами конфиденциальности в ГОСТ ISO/IEC 29100 для общедоступной облачной вычислительной среды
[13]	Предоставляет описание методов обезличивания данных, повышающих конфиденциальность, которые будут использоваться для описания и разработки мер обезличивания в соответствии с принципами конфиденциальности в ГОСТ ISO/IEC 29100. Определяет терминологию, классификацию методов обезличивания в соответствии с их характеристиками и их применимость для снижения риска повторной идентификации
ГОСТ Р ИСО/МЭК 27036-4	Предоставляет клиентам и поставщикам облачных служб руководство: - по получению информации о рисках информационной безопасности, связанных с использованием облачных сервисов, и эффективному управлению этими рисками; - по реакции на риски, связанные с приобретением или предоставлением облачных услуг, которые могут повлиять на информационную безопасность организаций, использующих эти службы

Справочная информация о дополнительных стандартах в области облачных вычислений приведена в приложении Б.

7.2 Стандарты серии «Информационные технологии. Облачные вычисления. Структура соглашения об уровне обслуживания (SLA)», применимые к доверию и прозрачности

Серия стандартов «Информационные технологии. Облачные вычисления. Структура соглашения об уровне обслуживания (SLA)» определяет цели уровня облачных служб (SLO) и цели качества облачных служб (SQO), которые входят в состав соглашений об облачных службах. Такие SLO или SQO часто ссылаются на ГОСТ Р ИСО/МЭК 27018 касаемо операторов общедоступных облаков или на [7] для SLO или SQO управления данными, которые должны основываться на таксономии и спецификациях использования данных.

При разработке политик и методов с использованием описанных в них концепций разработчикам государственных и корпоративных политик важно понимать эти взаимосвязи.

8 Рекомендации по разработке политик

8.1 Рекомендации по регуляторной политике

8.1.1 Общие положения

В настоящем разделе приведены обоснованные рекомендации по разработке политики, которая будет законно действовать при развертывании, предоставлении или использовании облачных служб.

Для удобства ссылок вопросы политики пронумерованы последовательно. Порядок изложения вопросов и рекомендаций не связан ни с их приоритетами, ни с их предпочтениями.

Поставщики облачных служб, как правило, предоставляют своим клиентам, партнерам и регулирующим органам значительный объем документации. В описаниях систем облачных вычислений не должно быть отклонений от принятых национальных, межгосударственных и международных норм и правил. Следует ответить на следующие вопросы:

а) Использует или определяет политика термины облачных вычислений, противоречащие определениям, содержащимся в 6.2, а также в ГОСТ ISO/IEC 17788 и [8]?

б) Всегда ли эта политика, где это возможно, ссылается на национальные, межгосударственные и международные стандарты определений (см. 6.2)?

в) Предотвращает ли эта политика непредвиденные инженерные последствия или смягчает их последствия посредством проведения обоснованных обсуждений в отрасли до внесения изменений в политику?

г) Содержит ли эта политика какие-либо временные ограничения и сроки реализации? Соответствуют ли они инженерным задачам реализации требований?

8.1.2 Проблемы многопользовательского использования

Как описано в 6.4.7, облачные службы обеспечивают экономию за счет масштаба и за счет разделения ресурсов между несколькими потребителями/пользователями.

Для коллективного доступа следует учитывать:

а) Требует ли политика, чтобы поставщики облачных служб предоставляли физический доступ к данным или системам государственным должностным лицам? Если да, то как она защищает права, такие как, например, конфиденциальность, целостность, доступность других пользователей облачных служб, размещенных в тех же физических системах или хранилищах данных, что и целевой объект (см. 6.4.7)?

б) Распространяется ли политика на удаление данных? Если да, то учитывает ли она потребности других пользователей, чьи данные хранятся на том же носителе (см. 6.4.7)?

в) Учитывает ли она финансовые затраты на уничтожение исправных носителей информации до окончания срока их службы (см. 6.4.3)?

г) Распространяется ли политика на права потребителя облачных служб на получение своих данных от поставщика облачных служб? Если да, то учитывает ли эта политика обработку ПДн других людей, которые могут содержаться в данных потребителя?

8.1.3 Устранение ненужных барьеров для внедрения облачных технологий

Политики, изначально разработанные для регулирования локальных вычислительных систем или локально размещенных систем, иногда могут препятствовать развертыванию эффективных архитектур облачных вычислений.

Следует рассмотреть следующие вопросы:

а) Включает ли политика в себя явные или неявные предположения или требования к сотрудникам поставщика облачных служб, такие как их гражданство или местонахождение (см. 6.4.2)?

б) Требует ли данная политика особых квалификаций местного персонала или разрешений, которые затруднили бы или сделали невозможным функционирование или управление персоналом поставщика облачных служб, базирующимся в другой юрисдикции (см. 6.4.2)?

в) Ограничивает ли политика способность поставщика облачных служб перемещать данные поставщика облачных служб (см. ГОСТ Р ИСО/МЭК 19941) между юрисдикциями (см. 6.4.2 и 6.4.3)?

г) Ограничивает ли политика место хранения данных клиентов облачных служб или производных данных конкретной юрисдикцией (см. 6.4.2)? Если да, то применяется ли это ограничение ко всем таким данным или к определенному подмножеству категорий данных? Если нет, то соответствуют ли эти категории данных таксономии данных, определенной в [7]?

д) Если политика включает ограничения на размещение данных, допускает ли она операционные исключения в особых обстоятельствах, например поддержание работы облачной службы во время серьезной чрезвычайной ситуации, затрагивающей локальные облачные центры обработки данных?

е) Соответствует ли политика стандартам управления ИТ (см. ГОСТ Р ИСО/МЭК 38500)?

ж) Допускает ли политика непрерывное развитие облачных служб и подключенных приложений (см. 6.4.6)?

и) Допускает ли политика непрерывные создание прототипов, разработку, тестирование и развертывание?

к) Поощряет или сдерживает политика поставщика облачных служб и потребителя облачных служб поддержание своих систем в актуальном состоянии?

л) Требует ли политика повторной сертификации или повторного утверждения при изменении программного обеспечения? Если да, то сколько изменений допускается до того, как потребуется повторная сертификация или повторное утверждение?

8.1.4 Доверие и прозрачность

Потребители облачных служб должны доверять своим поставщикам облачных служб, и опыт показывает, что лучше всего установить и поддерживать доверительные отношения, обеспечивая правдивость и прозрачность в отношении предлагаемых услуг и их функционирования.

Следует рассмотреть следующие вопросы:

а) Поощряет ли политика или требует использования в описаниях онлайн-вычислительных служб (облачных или иных) терминологии, установленной стандартами?

б) Запрещает ли политика использование таких терминов, как «облако» или «облачные вычисления», для описания услуг, которые не соответствуют стандартному определению облачных вычислений, определенному в ГОСТ ISO/IEC 17788?

в) Требует ли политика информирования потребителей облачных служб о том, как поставщик облачных служб будет использовать данные клиентов или производные данные? Если да, то требует ли политика или поощряет поставщика облачных служб предоставлять спецификации использования данных, построенные в соответствии со стандартным методом, определенным в [7]?

г) Требует ли политика использования стандартной терминологии в соглашениях об услугах облачных вычислений или соглашениях об уровне обслуживания (SLA)? Если да, то соответствует ли политика стандартной терминологии и структуре, определенным в ГОСТ Р ИСО/МЭК 19086-1?

8.1.5 Совместимость и переносимость

Функциональная совместимость и переносимость являются важными вопросами для потребителей облачных служб и регулирующих органов, особенно для тех из них, кто имеет дело с конкуренцией между поставщиками услуг. Вопросы совместимости и переносимости являются сложными, поэтому к ним следует подходить осторожно.

Следует ответить на следующие вопросы:

а) Охватывает ли политика вопросы совместимости или переносимости?

б) Разъясняет ли политика различия между (см. ГОСТ Р ИСО/МЭК 19941):

1) совместимостью;

2) переносимостью данных;

3) переносимостью приложений?

в) Учитывает ли политика конкретные аспекты взаимодействия или переносимости? Если да, согласованы ли эти аспекты с ГОСТ Р ИСО/МЭК 19941 или определены с использованием [7]?

г) Требует ли политика прямой совместимости (см. ГОСТ Р ИСО/МЭК 19941) или она также допускает использование таких средств, как:

1) конвертеры протоколов;

2) промежуточные форматы;

3) сторонние инструменты преобразования данных (например, с открытым исходным кодом);

4) другие решения?

д) Требует ли политика прямой переносимости данных или также позволяет использовать такие инструменты, как:

1) промежуточные форматы;

2) сторонние преобразователи (например, с открытым исходным кодом);

3) другие решения?

е) Требует ли политика прямой переносимости приложений или позволяет использовать такие дополнительные инструменты, как:

1) эмуляторы;

2) преобразователи кода приложения;

3) другие решения?

8.1.6 Безопасность и конфиденциальность

Уверенность в информационной безопасности и защите личной информации в облачных службах является необходимым условием для успешного внедрения технологий облачных вычислений.

Следует рассмотреть следующие вопросы:

а) Налагает ли политика особые требования безопасности на поставщиков и потребителей облачных служб?

б) Признает ли политика концепцию ответственности за обеспечение безопасности и конфиденциальности данных, выполняемой совместно поставщиком облачных служб и потребителем облачных служб?

в) Обеспечивает ли политика развитие технологий и методов обеспечения безопасности по мере появления новых угроз?

г) Предусматривает ли политика использование надежного шифрования данных в хранилищах и во время передачи?

д) Обеспечивает ли политика использование проверенных подходов к управлению рисками для обеспечения безопасности и конфиденциальности, которые описаны в ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27017, ГОСТ Р ИСО/МЭК 27018?

8.2 Советы по рекомендательной политике

8.2.1 Общие положения

В настоящем подразделе рассматриваются важные при разработке политики соображения, которые предоставляют рекомендации по использованию облачных вычислений, но не налагают обязательных требований.

Примерами такой политики могут быть случаи, когда государственные органы власти предоставляют руководящие принципы и рекомендации по использованию облачных служб местным органам власти или государственным учреждениям, но окончательные решения о том, использовать ли облачные службы и если использовать, то как, остаются за последними.

При разработке политики, которая будет содержать советы и/или рекомендации по развертыванию, предложениям или использованию облачных служб в юрисдикции, следует учитывать далее перечисленные соображения.

Для удобства ссылок вопросы политики пронумерованы последовательно. Порядок изложения вопросов и рекомендаций не связан ни с их приоритетами, ни с предпочтениями.

8.2.2 Содействие внедрению облачных технологий

Многие правительства видят преимущества перехода на соответствующие способы реализации облачных вычислений в ИТ для бизнеса, общества и окружающей среды, которые приведены в 6.3, и часто дают местным органам власти и учреждениям соответствующие рекомендации.

Следует рассмотреть следующие вопросы:

а) Рекомендует ли политика ориентированный на облачные технологии подход, отдавая приоритет использованию общедоступных облачных служб в тех ситуациях, когда эти технологии технически способны удовлетворить требованиям политики и организации?

б) Предоставляет ли политика местным органам власти или учреждениям рекомендации по критериям определения целесообразности внедрения облачных вычислений для своих ИТ-нужд?

в) Дает ли политика рекомендации по экологическим преимуществам перехода к технологиям, основанным на облачных вычислениях?

8.2.3 Терминология и таксономия

Правильная интерпретация рекомендательной политики зависит от общего понимания используемой терминологии и правильного определения категорий данных, к которым она будет применяться.

Следует рассмотреть следующие вопросы:

а) Использует ли эта рекомендательная политика терминологию стандартов облачных вычислений, определенную в ГОСТ ISO/IEC 17788 (см. также [3])?

б) Дает ли политика только общие рекомендации для определенных категорий или классификаций данных, типов приложений и целей или же предоставляет для них конкретные рекомендации (см. [7])?

8.2.4 Принятие малыми и средними предприятиями

Политика, разработанная в первую очередь для крупных предприятий и крупных операторов, поставщиков облачных служб, в отдельных случаях может налагать непропорциональное бремя на небольшие организации.

Необходимо получить ответы на вопросы:

а) Рекомендательная политика помогает или, наоборот, затрудняет использование облачных вычислений для небольших реализаций, таких как небольшие местные органы власти, образовательные учреждения или небольшие организации?

б) Рекомендательная политика поощряет или препятствует внедрению облачных вычислений теми малыми и средними предприятиями, которые предоставляют или выполняют работу для государства и организаций?

8.2.5 Сертификаты поставщиков

Соблюдать рекомендательную политику проще, если она содержит четкие указания по типам сертификатов, которые можно использовать для подтверждения полного или частичного соответствия.

Необходимо определить, дает ли рекомендательная политика указания относительно типов сертификатов, которые можно ожидать от поставщиков и подрядчиков, предлагающих облачные службы государству и учреждениям? Если да, то определяет ли эта политика надлежащие сертификаты соответствия стандартам, например перечисленным в разделе 7?

8.2.6 Сетевое подключение

Использование облачных вычислений подразумевает достаточную доступность соответствующей сети, будь то общедоступная сеть Интернет или какая-либо частная сеть.

Следует рассмотреть следующие вопросы:

а) Содержатся ли в политике рекомендации по сетевым вопросам как важным для преимуществ облачных вычислений? Если да, то поощряет ли политика обеспечение достаточного и надлежащего подключения к широкополосной сети и его доступности и надежности?

б) Предоставляет ли политика руководство по соответствующим вопросам разграничения ответственности потребителей облачных служб, поставщиков облачных служб, как операторов данных и поставщиков сетевых подключений?

8.2.7 Совместимость и переносимость

Обеспечение функциональной совместимости и переносимости часто упоминается как необходимое условие свободной рыночной конкуренции между поставщиками ИТ-услуг, включая облачные вычисления.

Следует рассмотреть вопрос: предоставляет ли политика руководство по типам совместимости или переносимости, к которым следует стремиться? Если да, то адекватно ли формулирует политика сложность совместимости и переносимости и соответствует ли политика структуре международных стандартов, представленной в ГОСТ Р ИСО/МЭК 19941?

8.3 Рекомендации по политике закупок

В настоящем подразделе рассматриваются соображения, имеющие особое значение при разработке политик закупок для покупателей и пользователей облачных служб, независимо от того, приобретаются ли они государством, государственными учреждениями или коммерческими предприятиями.

Примерами могут служить случаи, когда государство, предприятие, департамент или другой потребитель облачных служб устанавливает правила, которые будут определять, ограничивать или контролировать облачные службы, которые могут приобретаться и использоваться их отделами и сотрудниками.

Далее изложены аспекты, которые следует учитывать при разработке политики, содержащей советы и/или рекомендации по покупке, развертыванию, предложению или использованию облачных служб в организации.

Для удобства ссылок аспекты политики пронумерованы последовательно. Порядок изложения вопросов и рекомендаций не связан ни с их приоритетами, ни с предпочтениями.

8.3.1 Терминология и таксономия

Некоторые поставщики облачных вычислений и другие поставщики ИТ в своих маркетинговых материалах или описаниях продуктов иногда используют терминологию, которая отличается от принятых в международных стандартах терминов или которая менее понятна. Для политики закупок крайне важно, чтобы используемые термины понимались и использовались одинаково всеми поставщиками в их предложениях услуг.

Необходимо ответить на следующие вопросы:

а) Использует ли эта политика закупок стандартную терминологию облачных вычислений в соответствии с ГОСТ ISO/IEC 17788, другими национальными и межгосударственными стандартами (см. также [3])?

б) Руководствуется ли эта политика закупок ГОСТ Р ИСО/МЭК 19086-1 и ГОСТ Р ИСО/МЭК 19086-4 в части терминов и концепций соглашения об облачных службах?

в) Если эта политика закупок налагает ограничения на использование данных клиентов или производных данных поставщиком облачных служб, то определяет ли она категории таких данных в соответствии с таксономией, описанной в [7]?

8.3.2 Модели развертывания облачных служб

Существуют различные способы получения облачных служб, и политика закупок должна обеспечивать рассмотрение всех подходящих моделей развертывания служб.

Необходимо рассмотреть следующие вопросы:

а) Ограничивает ли эта политика закупок поставщиков какой-либо конкретной моделью или моделями развертывания (например, частным облаком, общедоступным облаком, облаком сообщества или гибридным облаком — см. ГОСТ ISO/IEC 17788)? Если да, то было ли это ограничение оправдано другими конкретными требованиями?

б) Имеет ли поставщик свободу предлагать альтернативные модели развертывания, если он может показать, что они могут соответствовать другим специальным требованиям?

8.3.3 Сертификаты поставщиков

В политике закупок облачных вычислений должны быть четко указаны все сертификаты, которые должен иметь поставщик облачных служб.

Следует рассмотреть вопрос: определяет ли эта политика закупок сертификаты, которые ожидаются от поставщика облачных служб и подрядчиков? Если да, то ссылается ли эта политика на сертификацию, основанную на стандартах, перечисленных в разделе 7?

8.3.4 Совместимость и переносимость

Обеспечение функциональной совместимости и переносимости часто упоминается как необходимое условие свободной рыночной конкуренции между поставщиками ИТ-услуг, включая облачные вычисления.

Следует рассмотреть следующие вопросы:

а) Требует ли эта политика особых функций совместимости или переносимости? Если да, то определены ли эти функции с точки зрения концепций и структуры, описанных в ГОСТ Р ИСО/МЭК 19941?

б) Если требуются возможности функциональной совместимости или переносимости, учитываются ли в политике альтернативные инженерные механизмы для достижения желаемой цели (например, предложенные в 8.1.5)?

9 Выводы

Настоящий стандарт содержит:

- объяснение технических аспектов облачных вычислений, которые имеют значение для разработки политики;
- выделение ряда национальных и межгосударственных стандартов, которые рекомендовано использовать для упрощения и ускорения разработки такой политики;
- рекомендации по разработке политики облачных вычислений.

Настоящий стандарт направлен на формирование представлений о том, что использование национальных и межгосударственных стандартов при разработке политик облачных вычислений сделает процессы разработки такой политики более простыми и последовательными, а также упростит реализации таких политик поставщиками облачных служб. Таким образом, основанный на стандартах подход повысит прозрачность и конкуренцию, а также будет способствовать внедрению облачных служб в интересах клиентов облачных служб, государств и общества в целом.

Приложение А
(справочное)

Взаимосвязь между ключевыми характеристиками и выводами

В таблице А.1 приведены ключевые характеристики облачных вычислений в соответствии с ГОСТ ISO/IEC 17788, их описание и выводы.

Таблица А.1 — Взаимосвязь между ключевыми характеристиками и последствиями

Ключевые характеристики облачных вычислений в соответствии с ГОСТ ISO/IEC 17788	Описание	Выводы
Широкий доступ к сети	Функция, при которой физические и виртуальные ресурсы доступны через стандартные механизмы сети, которые обеспечивают их использование различными клиентскими устройствами и приложениями	См. 6.2.2, 6.4.4, 6.4.8, 6.4.10, 6.4.12, 6.4.14, 8.1.6, 8.2.5
Измеренное обслуживание	Измеренное предоставление облачных услуг, позволяющее отслеживать использование, контролировать его, создавать отчеты и выставлять счета	См. 6.2.2, 6.4.4, 6.4.6, раздел 7
Многопользовательский доступ	Распределение физических или виртуальных ресурсов таким образом, что несколько пользователей, их вычисления и данные были изолированы и недоступны друг другу	См. 6.2.2, 6.4.2, 6.4.7, 6.4.11, 7.1.1, 8.1.2, 8.1.4, 8.1.6
Самообслуживание по требованию	Функция, при которой потребитель облачных служб может при необходимости получать вычислительные возможности автоматически или с минимальным взаимодействием с поставщиком облачных служб	См. 6.2.2, 6.3.1, 6.4.2, 6.4.3, 6.4.4, 6.4.5
Оперативная гибкость и масштабируемость	Функция, в которой физические или виртуальные ресурсы могут быть быстро и гибко настроены, в некоторых случаях автоматически, для быстрого увеличения или уменьшения ресурсов	См. 6.2.2, 6.4.2, 6.4.3, 6.4.4, раздел 7
Пул ресурсов	Агрегация физических или виртуальных ресурсов поставщика облачных служб для обслуживания одного или нескольких потребителей облачных служб	См. 6.2.2, 6.3.1, 6.4.2, 6.4.3, 6.4.7, 6.4.10, раздел 7, 8.1.5, 8.2.6, 8.3.4

Приложение Б
(справочное)

Дополнительные стандарты

В дополнение к стандартам, указанным в настоящем стандарте, рекомендуются следующие стандарты разработчикам политик для облачных вычислений.

Таблица Б.1 — Дополнительные стандарты в области облачных вычислений

Стандарт	Описание
[14]	Устанавливает требования доступности для государственных закупок продуктов и услуг ИКТ в Европе
[15]	Описывает шифрование с аутентификацией
Серия стандартов «Информационные технологии. Управление услугами»	Информационные технологии. Менеджмент услуг
ГОСТ Р ИСО/МЭК 27050-1	Информационные технологии. Методы обеспечения безопасности. Выявление и раскрытие электронной информации
ГОСТ ISO/IEC 29100	Основы обеспечения приватности
ГОСТ Р ИСО/МЭК 30134-2	Определяет стандартный показатель эффективности использования энергии (PUE) для центров обработки данных облачных вычислений
[16]	Определяет использование ИТ-оборудования для отдельных серверов в качестве ключевого показателя производительности (KPI) для повышения совокупной энергоэффективности серверов в центре обработки данных
ГОСТ Р ИСО/МЭК 38500	Определяет стратегическое управление ИТ в организации
[17]	Расширяет ГОСТ Р ИСО/МЭК 38500 для менеджмента данных
[18]	Руководство по обеспечению доступности веб-контента (WCAG) 2.0 охватывает широкий спектр рекомендаций по повышению доступности веб-контента. Следование этим рекомендациям сделает контент доступным для более широкого круга людей с ограниченными возможностями, включая слепоту и слабое зрение, глухоту и потерю слуха, нарушения обучаемости, когнитивные ограничения, ограниченное движение, нарушения речи, светочувствительность и их комбинации. При соблюдении рекомендаций веб-контент становится более удобным для пользователей. Обратите внимание, что WCAG 2.1 находится на заключительной стадии разработки в W3C, но еще не опубликован
[19]	Описывает потребности пользователей в доступном пользовательском интерфейсе
[20]	Предоставляет руководство по обеспечению доступности стандартов
[21]	Распространяет действие [17] на управление данными

Библиография

[1] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями на 2 июля 2021 г.)

[2] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями на 14 июля 2022 г.)

[3] ИСО/МЭК 22123-1:2021 Информационная технология. Облачные вычисления. Часть 1. Словарь (Information technology — Cloud computing — Part 1: Vocabulary)

[4] ITU-N X.1601 (2014) Безопасность облачных вычислений. Обзор безопасности облачных вычислений (Cloud Computing Security — Cloud Computing Security Framework)

[5] ИСО/МЭК 19395:2015 Информационная технология. Устойчивость для ИТ и с помощью ИТ. Контроль и управление интеллектуальными ресурсами центра обработки данных (Information technology — Sustainability for and by information technology — Smart data centre resource monitoring and control)

[6] ИСО/МЭК 30134-4:2017 Информационная технология. Центры данных. Ключевые показатели эффективности. Часть 4. Энергоэффективность информационно-технического оборудования для серверов (ITEEsv) [Information technology — Data centres — Key performance indicators — Part 4: IT Equipment Energy Efficiency for servers (ITEEsv)]

[7] ИСО/МЭК 19944-1:2020 Облачные службы и распределенные платформы. Поток данных, категории данных и их использование. Часть 1. Общие положения (Cloud computing and distributed platforms — Data flow, data categories and data use — Part 1: Fundamentals)

[8] ИСО/МЭК 17789:2014 Информационные технологии. Облачные вычисления. Эталонная архитектура (Information technology — Cloud computing — Reference architecture)

[9] ITU-T Y.3501 (2016) Облачные вычисления. Инфраструктура и требования высокого уровня (Cloud computing — Framework and high-level requirements)

[10] ИСО/МЭК 19086-2:2018 Информационная технология. Облачные вычисления. Структура соглашения о качестве предоставляемых услуг (SLA). Часть 2. Метрическая модель [Information technology — Cloud Computing — Service Level Agreement (SLA) Framework — Part 2: Metric Model]

[11] ИСО/МЭК 19086-3:2017 Информационная технология. Облачные вычисления. Структура соглашения о качестве предоставляемых услуг (SLA). Часть 3. Базовое требование соответствия [Information technology — Cloud computing — Service level agreement (SLA) framework — Part 3: Core conformance requirements]

[12] ISO/IEC TS 23167:2020 Информационная технология. Облачные вычисления. Общие технологии и методы (Information technology — Cloud computing — Common technologies and techniques)

[13] ИСО/МЭК 20889:2018 Терминология и классификация методов идентификации данных повышенной конфиденциальности (Privacy enhancing data de-identification terminology and classification of techniques)

[14] ETSI EN 301 549 v3.2.1 (2021-03) Требования доступности к продукции и услугам информационно-коммуникационных технологий (Accessibility requirements for information and communication technology products and services)

[15] ИСО/МЭК 19772:2020 Защита информации. Аутентификационное шифрование (Information security — Authenticated encryption)

[16] ИСО/МЭК 30134-5:2017 Информационная технология. Центры данных. Ключевые показатели эффективности. Часть 5. Использование информационно-технического оборудования для серверов (ITEUsv) [Information technology — Data centres — Key performance indicators — Part 5: IT Equipment Utilization for servers (ITEUsv)]

[17] ИСО/МЭК 38505-1:2017 Информационная технология. Стратегическое управление ИТ. Стратегическое управление данными. Часть 1. Применение ИСО/МЭК 38500 для менеджмента данных (Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data)

[18] ИСО/МЭК 40500:2012 Информационные технологии. Руководящие указания 2.0 по доступности веб-содержания W3C [Information technology — W3C Web Content Accessibility Guidelines (WCAG) 2.0]

[19] ИСО/МЭК 29138-1:2018 Информационная технология. Доступность интерфейса пользователя. Часть 1. Требования к доступности пользователя (Information technology — User interface accessibility — Part 1: User accessibility needs)

[20] ISO/IEC Guide 71:2014 Руководство по решению в стандартах вопросов создания доступной среды (Guide for addressing accessibility in standards)

[21] ISO/IEC TR 38505-2:2018 Информационная технология. Стратегическое управление ИТ. Стратегическое управление данными. Часть 2. Последствия применения ИСО/МЭК 38500 для менеджмента данных (Information technology — Governance of IT — Governance of data — Part 2: Implications of ISO/IEC 38500 for data management)

УДК 006.034:004.77:004.6:006.354 ОКС 35.210

Ключевые слова: политики, категории данных, поставщик облачной службы, потребитель облачных служб, таксономия, соглашение об уровне обслуживания

Редактор *Е.В. Якубова*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *М.В. Малеевой*

Сдано в набор 18.08.2022. Подписано в печать 25.08.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 2,98.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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