ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 70289— 2022

Информационные технологии

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ

Особенности обработки различных категорий данных в облачных службах

(ISO/IEC 22624:2020, 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 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 17 августа 2022 г. № 780-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта ISO/IEC 22624:2020 «Информационные технологии. Облачные вычисления. Таксономия на основе обработки данных для облачных служб» (ISO/IEC 22624:2020 «Information technology — Cloud computing — Taxonomy based data handling for cloud services», 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

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Сокращения 3
5 Необходимость структурированного представления политик и практик, основанных на общей таксономии данных 3
6 Основы структурированного представления связанных с данными политик и методов 4
6.1 Общие положения 4
6.2 Элементы структуры 4
7 Использование структуры 11
7.1 Режимы использования структуры 11
7.2 Использование структурных элементов 11
7.3 Представление политик 11
7.4 Пример 12
8 Представление политик данных для конкретных проблемных областей 12
8.1 Общие положения 12
8.2 Размещение данных 13
8.3 Трансграничная передача данных 13
8.4 Переносимость данных и доступ к данным 17
8.5 Использование данных 19
8.6 Управление данными 19
8.7 Корпоративное управление данными 23
9 Применение структуры к кодексам поведения 28
Приложение А (справочное) Пример использования настоящего стандарта 34
Библиография 48

Введение

Большинство политик и методов, применяемых для обработки данных в экосистеме облачных вычислений, необходимо определять на основе категорий обрабатываемых данных. Например, информация, позволяющая установить личность, — персональные данные (ПДн), — предъявляет особые требования к управлению данными не только с точки зрения безопасности, но и в отношении механизмов, которые позволяют пользователям облачных сервисов осуществлять контроль над использованием и передачей таких данных. Организационные данные, такие как информация об использовании облачных сервисов и данные телеметрии облачных сервисов, могут использоваться для операционных целей, таких как улучшение качества обслуживания, и соответствовать определенным требованиям к качеству.

Данные контента клиента могут быть связаны с правами на результаты интеллектуальной деятельности и, возможно, требуют соответствующей защиты со стороны поставщика облачных служб (CSP). Некоторые данные могут передаваться из одной юрисдикции в другую. В зависимости от категории данных к передаче и обработке информации предъявляют различные требования, установленные действующими нормативными правовыми документами (международные договоры Российской Федерации, федеральные законы, акты Президента Российской Федерации, акты Правительства Российской Федерации, нормативные правовые акты федеральных органов исполнительной власти, нормативные правовые акты регуляторов), регулирующими передачу и обработку.

Политики и методы передачи и обработки данных целесообразно определять в структурированном и последовательном виде с тем, чтобы стороны, заинтересованные в экосистеме облачных вычислений, могли бы их лучше представлять, оценивать, анализировать и сопоставлять. В [1] представлена исчерпывающая таксономия, определяющая детализированную систему категорий данных, которая может применяться к различным областям политик обработки данных в экосистеме облачных вычислений, таким как трансграничная передача данных, размещение, использование данных, доступ к данным, перенос данных и управление данными, включая управление качеством данных и безопасностью данных, или корпоративное управление данными. Кроме того, в [1] представлены рекомендации по определению политик и методов обработки данных в кодексах поведения.

В настоящем стандарте описывается общий структурированный подход для представления различных политик и методов обработки данных. Важно подчеркнуть, что сами политики и практики выходят за рамки настоящего стандарта. Для того чтобы понять, как использовать [1] при применении политик и анализе их требований, в настоящем стандарте представлен ряд примеров из области обработки данных.

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ

Особенности обработки различных категорий данных в облачных службах

Information technology. Cloud computing. Features of processing different categories of data in cloud services

Дата введения — 2023—03—30

1 Область применения

В настоящем стандарте представлено:

- определение основ структурированного представления связанных с данными политик и практик в области облачных вычислений на основе таксономии данных с учетом [1];
- руководящие принципы по применению таксономии для обработки данных на основе разделения на категории и классификации данных;
- определение политик и практик, связанных с данными, включая, помимо прочего, размещение данных, трансграничную передачу данных, доступ к данным, переносимость данных, использование данных, управление данными, а также корпоративное управление данными;
- описание того, как основы могут быть использованы в кодексах поведения для хранения и передачи данных, включая трансграничную передачу данных, а также удаленный доступ к данным;
- варианты использования для задач обслуживания данных, то есть контроля, доступа и определения местоположения данных в соответствии с категориями данных (см. [1]).

Настоящий стандарт предназначен в первую очередь для поставщиков облачных услуг, потребителей и пользователей облачных служб, а также для всех лиц или организаций, интересы которых включают юридические, политические, технические или другие аспекты управления данными на основе таксономии в облачных услугах.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ Р ИСО 13008 Информация и документация. Процессы конверсии и миграции электронных документов

ГОСТ Р ИСО/МЭК 19941—2021 Информационные технологии. Облачные вычисления. Интероперабельность и переносимость

ГОСТ Р ИСО/МЭК 27000 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

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

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 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, ГОСТ Р ИСО/МЭК 27000[1)], а также следующие термины с соответствующими определениями:

3.1 **кодексы поведения** (codes of conduct): Согласованный набор моделей поведения между организациями для улучшения взаимодействия с клиентами и/или партнерами.

3.2

конфиденциальность (confidentiality): Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателей.

[[2], статья 2]

3.3 **целостность** (integrity): Свойство сохранения правильности и полноты активов.

3.4 **доступность** (availability): Свойство, определяющее возможность использования объекта авторизованным субъектом по запросу.

3.5

доступ к данным (data access): Возможность получения информации и ее использования.

[[2], статья 2]

3.6 **передача данных** (data transfer): Копирование или перемещение данных из одной системы в другую.

3.7 **размещение данных** (data geolocation): Географическое положение хранения объекта данных.

3.8

обезличивание персональных данных (personally identifiable information anonymization): Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

[[3], статья 3]

3.9 **псевдонимизированные данные** (pseudonymized data): Данные, для которых все идентификаторы заменены псевдонимами, причем присвоение псевдонимов таково, что обратное преобразование не может быть выполнено разумными усилиями кого-либо, кроме стороны, которая выполнила присвоение псевдонима.

3.10 **анонимизированные данные** (anonymized data): Данные, полученные в результате обезличивания без возможности обратного действия.

[1)] См. также [1].

3.11

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

[[3], статья 3]

3.12 **обработчик данных** (data processor): Лицо, обрабатывающее 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:

ИИ — искусственный интеллект;

ИТ — информационные технологии;

ПДн — персональные данные;

ПК — персональный компьютер;

ПО — программное обеспечение;

СМИБ — система менеджмента информационной безопасности;

API — программный интерфейс приложения (Application Program Interface);

CSC — потребитель облачной службы (Cloud Service Customer);

CSN — партнер облачной службы (Cloud Service Partner);

CSP — поставщик облачной службы (Cloud Service Provider);

DRM — управление цифровыми правами (Digital Rights Management);

EUII — идентифицирующая информация конечного пользователя (End User Identifiable Information);

HBI — высокое влияние на бизнес (High Business Impact);

IRM — управление информационными правами (Information Rights Management);

LBI — низкое влияние на бизнес (Low Business Impact);

MBI — среднее влияние на бизнес (Medium Business Impact);

SaaS — программное обеспечение как услуга (Software as a Service);

OII — идентифицирующая информация организации (Organization Identifiable Information).

5 Необходимость структурированного представления политик и практик, основанных на общей таксономии данных

Политика и практика обработки данных на корпоративном или государственном уровне должны быть сформулированы с необходимой степенью точности и ясности. Необходимость определенной степени точности, наряду с необходимостью эффективного сравнения и анализа различных политик, требует общего и структурированного, основанного на общей таксономии данных подхода к представлению таких политик и практик.

В [1] представлен исчерпывающий набор элементов, которые можно использовать для следующих действий:

а) присвоение заданному набору информации категории данных, например персональные данные (ПДн), идентифицирующая информация организации, данные контента клиента и пр.;

б) определение классов действий, применяемых к таким данным, например использование для предоставления услуги, ее оптимизации, использование для маркетинга и пр.;

в) определение уровня использования данных, например уровень сервиса, уровень предприятия, организационный уровень или уровень использования третьими лицами;

г) определение уровня обезличивания (или анонимности), применяемого к набору данных, соответствующего одному из квалификаторов, как «идентифицируемый», «анонимизированный», «псевдонимизированный», «агрегированный» и пр.

Далее в настоящем стандарте для ссылки на данные элементы используются термины: «категории данных», «таксономия данных», «действия», «области действия» и «квалификаторы». В разделе 6 представлен исчерпывающий обзор элементов.

Чтобы определить политики и методы обработки данных для конкретного приложения, необходимо применить эти элементы к области, аналогичной или близкой к области приложения, включая классификацию данных относительно уровней безопасности или рисков, применимых к данным, а также техническую и организационную квалификацию данных. Таким образом, подход, описанный в настоящем стандарте, требует анализа категорий данных (см. 1]), а также анализа ортогональной информации, зависящей от конкретного рассматриваемого приложения. В связи с этим в примерах, используемых для пояснения этого подхода, используется формат табличного представления, который подчеркивает ортогональный характер общей категоризации данных (строки) и элементов, специфичных для приложения (колонки). Такой формат обеспечивает разработчиков корпоративных политик использования данных полноценной картиной всех аспектов, которые необходимо учитывать при разработке политик.

Неперсональные данные определяются как данные, которые не являются личными и не входят в состав ПДн, например научные данные, данные о продажах и т. д. Смешанные наборы данных включают в себя как ПДн, так и неперсональные данные, такие как данные о человеческих ресурсах, которые содержат организационные структуры и данные, принадлежащие сотрудникам. Важно осознавать различие таких наборов, поскольку к каждому из них могут применяться разные политики и методы обработки. Настоящий стандарт рассматривает аспекты, связанные с ПДн, и не углубляется в вопросы, относящиеся к неперсональным или смешанным наборам данных.

Настоящий стандарт содержит следующие разделы:

- в разделе 6 определены основы структурированного представления политик и практик, связанных с данными, включая элементы структуры (см. [1]), что далее дополняется обсуждением классификации данных (см. 6.2.6);
- в разделе 7 представлено руководство по использованию структуры, определенной в разделе 6;
- в разделе 8 рассматривается использование структуры в конкретных проблемных областях;
- в разделе 9 описывается применение основ к кодексам поведения.

6 Основы структурированного представления связанных с данными политик и методов

6.1 Общие положения

В настоящем стандарте используется структура представлений таксономии и использования данных с учетом [1]. Каждая политика или практика, которая соответствует настоящему стандарту и использует представления таксономии или использования данных, рассматривается с учетом [1].

Для работы с ключевыми темами управления данными в разделе 6 описывается согласованная структура для представления предпочтительной политики управления данными на основе различных типов данных с использованием таксономии данных с учетом [1]. Политики управления данными, основанные на общей структуре, определенной в настоящем стандарте, можно точно отображать, сравнивать и обсуждать.

Важно отметить, что настоящий стандарт не определяет одну или несколько политик данных, он скорее предлагает общие основы и структуру, которыми можно воспользоваться для отображения выбранной политики.

Более того, в настоящем стандарте не оговаривается какой-либо конкретный формат или синтаксис, которые будут использоваться для представления политик и практик, связанных с категоризацией данных. Хотя таблицы часто используются в настоящем стандарте для иллюстрации использования структуры, использование табличных форматов не является нормативным или обязательным, а служит только для наглядного представления примеров.

6.2 Элементы структуры

6.2.1 Общие положения

В [1] определена совокупность элементов для представления спецификаций, которые описывают использование данных поставщиком облачной службы, а именно иерархию категоризации данных, набор квалификаторов, указывающих уровень обезличивания данных, и иерархию областей, которые опи-

сывают, на каком уровне данные собираются и обрабатываются поставщиком облачной службы, набор действий, используемых для обработки данных, и на каком уровне используется результат обработки данных. В этом разделе представлен обзор элементов, которые подробно описаны в [1].

6.2.2 Категории данных

6.2.2.1 Общие положения

Таксономия данных (см. [1]), как показано на рисунке 1, определяет четыре основные категории данных, а именно: данные контента клиента, производные данные, данные поставщика облачной службы и данные учетной записи.

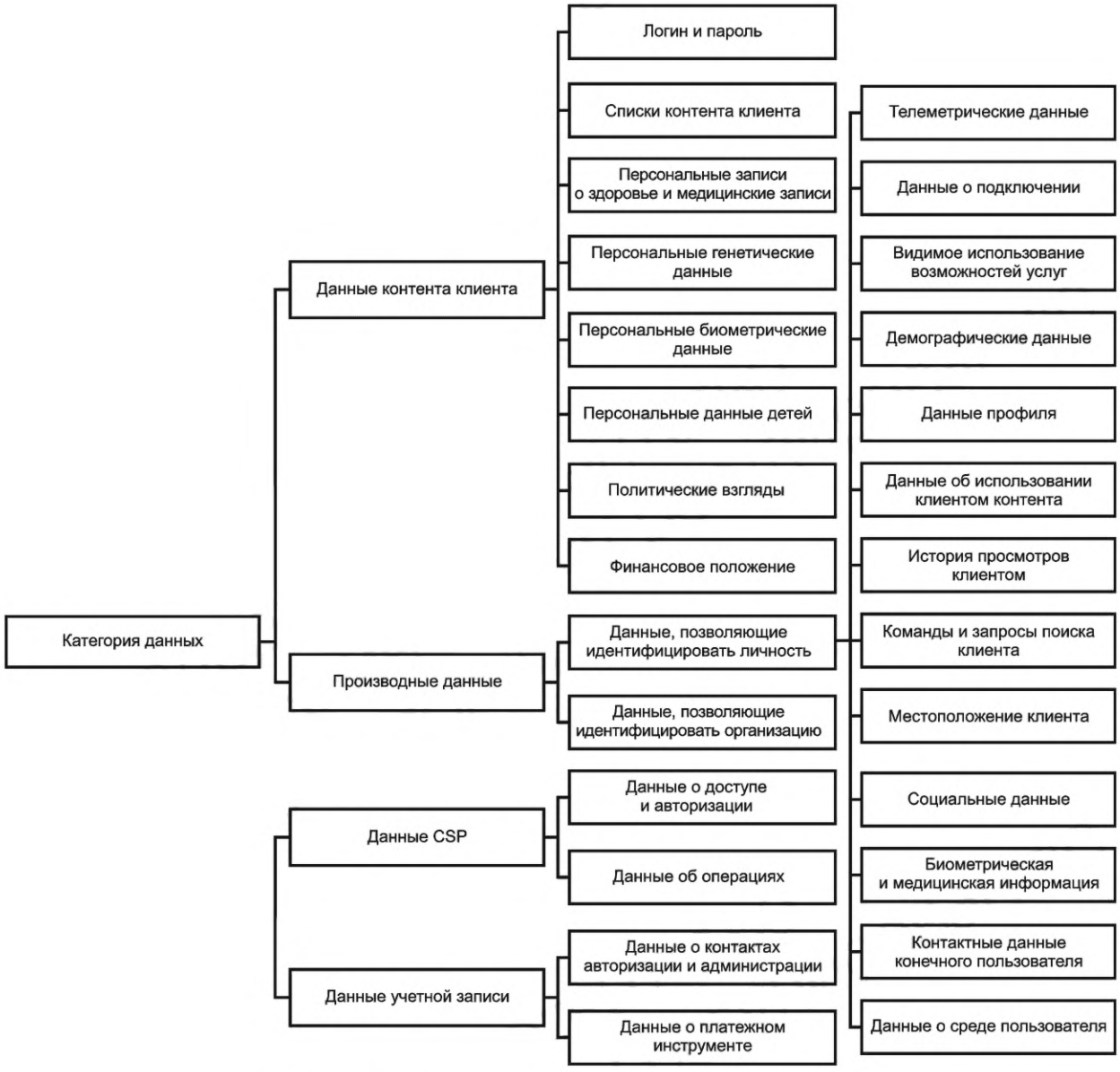

Рисунок 1 — Иерархия категоризации данных с учетом [1]

6.2.2.2 Данные контента клиентов

Данные контента клиента — это данные потребителя облачной службы (CSC), дополняющие соответствующие объекты данных, предоставляемых выполняющимися локально приложениями. Сюда входят контент, непосредственно созданный клиентами и их пользователями, и все данные, которые клиент предоставляет облачной службе или которые предоставляются облачной службе локальными службами или приложениями от имени клиента. Кроме того, сюда входят данные, которые пользователь

намеренно создает с помощью облачных приложений или службы. Эта категория данных содержит большое количество подкатегорий. Подробная информация приведена в [1], 8.2.2.

6.2.2.3 Производные данные

Производные данные — это данные, полученные из облачной службы, дополненные соответствующими объектами данных, предоставляемых выполняющимися локально приложениями пользователя.

Идентифицирующая информация конечного пользователя (EUII) определяется как связанные с конкретным пользователем данные, которые собираются или генерируются в результате использования службы этим пользователем. Идентифицирующую информацию конечного пользователя можно связать с конкретным пользователем, но в ней нет данных о контенте клиента. Эта категория данных включает в себя большое количество подкатегорий. Подробнее см. [1], 8.2.3.2.

Идентифицирующая информация организации (OII) — это данные, по которым можно идентифицировать конкретного клиента-организацию (общая конфигурация или данные об использовании), но которые не связаны с конкретным пользователем и не содержат информацию о контенте клиента. Сюда также входят данные, полученные от пользователей организации, но которые нельзя связать с отдельным пользователем.

6.2.2.4 Данные поставщика облачной службы

В эту категорию входят данные, которые контролируются исключительно поставщиком облачной службы. Эти данные уникальны для системы и находятся под контролем поставщика облачной службы.

Данные доступа и аутентификации — это данные, используемые в облачной службе для управления доступом к другим категориям данных или к возможностям службы.

Данные об операциях или операционные данные — это данные, которые используются для поддержки работы поставщика облачной службы и обслуживания системы, такие как журналы обслуживания, техническая информация о подписках (например, топология службы), техническая информация о клиенте (например, специализация клиента), параметры/файлы конфигурации.

6.2.2.5 Данные учетной записи

Данные учетной записи — это класс данных, специфичных для каждого потребителя облачной службы. Эти данные необходимы для регистрации, покупки или администрирования облачной службы. Сюда включена такая информация, как имена, адреса, информация для платежей. Данные учетной записи обычно находятся под контролем поставщика облачной службы, хотя каждый потребитель облачной службы обычно имеет возможность вводить, читать и редактировать информацию собственной учетной записи, но не учетные записи других потребителей облачной службы.

6.2.3 Квалификаторы идентификации данных

Информацию, которая идентифицирует конкретную личность или которая может быть связана, получают из данных практически любой категории. Степень возможности непосредственной идентификации личности и то, насколько легко связать набор характеристик в данных с конкретным лицом, определяется набором квалификаторов, показанных на рисунке 2.

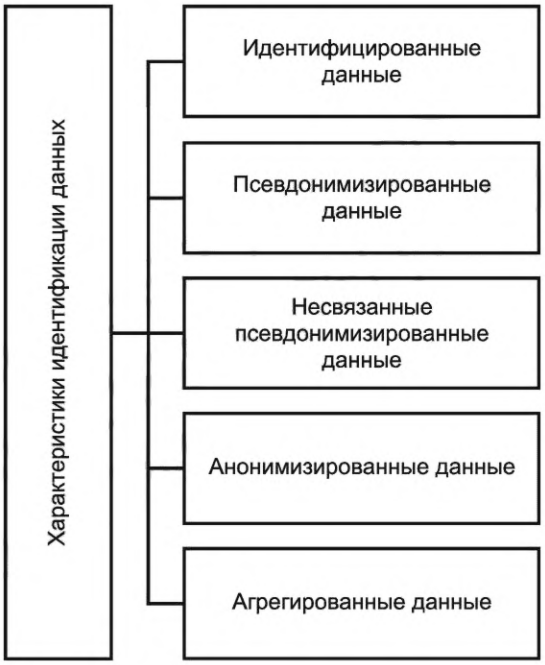

Рисунок 2 — Квалификаторы идентификации данных с учетом [1]

Идентифицированные данные. Данные, которые могут быть однозначно связаны с конкретным лицом, потому что в информации можно найти ПДн.

Псевдонимизированные данные. Данные, для которых все идентификаторы заменены псевдонимами, причем присвоение псевдонимов таково, что обратное преобразование не может быть выполнено разумными усилиями кого-либо, кроме стороны, которая выполнила присвоение псевдонима.

Несвязанные псевдонимизированные данные. Данные, для которых все идентификаторы удалены или заменены псевдонимами, причем функция присвоения псевдонимов недоступна или необратима, то есть обратное преобразование не может быть выполнено разумными усилиями кого-либо, включая сторону, которая выполнила присвоение псевдонима.

Анонимизированные данные. Несвязанные данные, атрибуты которых изменены таким образом, что имеет место разумный уровень уверенности в том, что лицо не может быть идентифицировано прямо или косвенно, по одним этим данным или в сочетании с другими данными.

Агрегированные данные. Статистические данные, которые не содержат записей индивидуального уровня и объединены с информацией о разных лицах, так что атрибуты индивидуального уровня не поддаются идентификации.

6.2.4 Области использования данных

Определение «области использования» (см. [1, пункт 9.4.1]) обеспечивает способ четкого описания границ сбора и использования данных в экосистемах облачных устройств и сервисов. Эти области можно использовать для описания приложений и служб, связанных с использованием данных (см. рисунок 3). Возможность — это составляющая приложения или одна из облачных служб, перечисленных в соглашении об обслуживании. Возможности входят в состав облачных служб, предоставляемых поставщиком облачной службы, и в подмножество общей совокупности продуктов и услуг поставщика облачной службы.

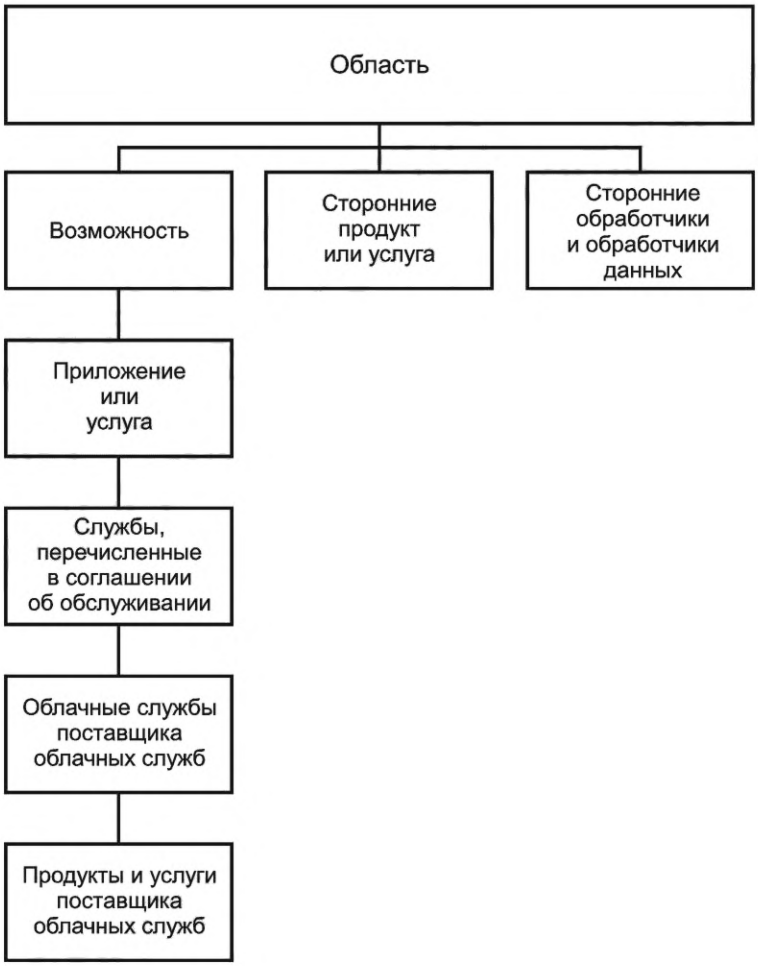

Рисунок 3 — Области использования данных (см. [1])

6.2.5 Действия

На рисунке 4 представлены возможные действия с данными.

Для данных различных категорий возможны следующие действия:

- предоставлять. Использовать данные для предоставления или защиты определенной услуги или возможности услуги, а также для предоставления клиенту информации о статусе и доступности возможностей;
- улучшать. Использовать данные для улучшения или повышения качества функциональных возможностей;
- персонализировать. Использовать данные для изменения представления возможностей или для изменения выбора и представления данных или рекламных акций, доступных с помощью этих возможностей, так, чтобы они были специфичными для пользователя, с учетом информации о пользователе;
- предлагать обновление или дополнительные возможности. Использовать данные, чтобы предложить заказчику увеличенную емкость, или ресурсы, или новые возможности в обмен на компенсацию;
- продавать, рекламировать, продвигать. Продвигать на рынке на основе данных определенные продукты и услуги пользователям или клиентам;
- делиться. Передавать данные объекту, отличному от поставщика облачной службы, изначально хранившего или обрабатывающего эти данные.

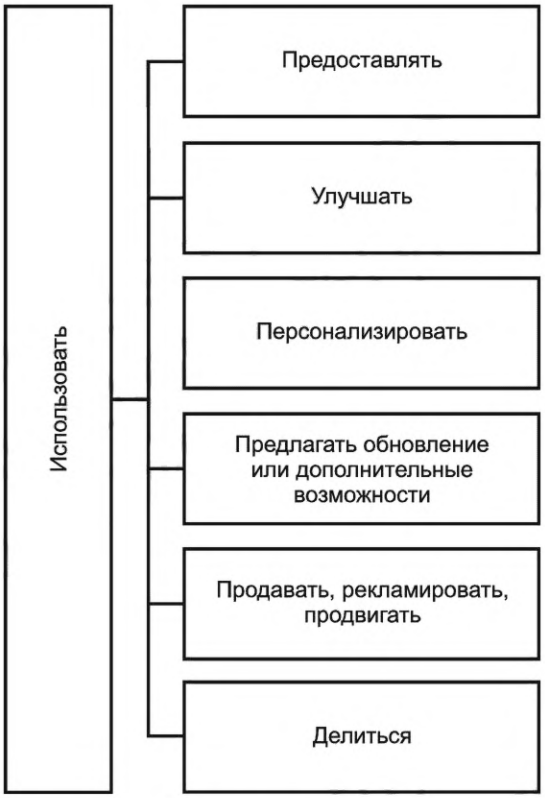

Рисунок 4 — Действия с данными с учетом [1]

6.2.6 Классификация данных

Классификация данных — это процесс организации данных в определенные классы для обеспечения безопасного, эффективного и действенного их использования. Процесс эффективной классификации данных, как правило, является частью стратегий процесса оценки и снижения рисков организации. Такая классификация, как правило, основана на потребностях в данных, подлежащих классификации, различных заинтересованных сторон, среди которых могут быть государственные регулирующие органы, внешние клиенты или поставщики и другие участники. Большинство организаций имеют дело с сетями поставщиков и клиентов, в которых возможно перемещение данных за пределы организации. В таких случаях необходимо, чтобы меры обеспечения безопасности в каждом пункте назначения соответствовали или превосходили меры обеспечения безопасности, предусмотренные в источнике информации.

Таким образом, классификация данных распределяет данные по классам на основе уровней чувствительности и воздействия на организацию в результате использования, раскрытия, изменения или уничтожения данных без надлежащих разрешений. Например:

- классификация данных с точки зрения информационной безопасности помогает определить набор соответствующих мер безопасности для защиты этих данных;
- классификация данных, позволяющих установить личность, с точки зрения защиты данных помогает организациям установить оценку воздействия на конфиденциальность для выявления рисков для отдельных лиц при обработке их ПДн.

Одна из проблем заключается в том, что класс данных может со временем меняться (то, что раньше считалось «общедоступным», может теперь стать «конфиденциальным»). Другой проблемой является соблазн «перестараться» с классификацией данных из-за опасений, связанных с возможным получением ПДн или других конфиденциальных данных на основе объединения неконфиденциальных атрибутов. Оценка вероятности раскрытия и воздействия раскрытия помогает классифицировать данные соответствующим образом. Использование соответствующих методов шифрования и токенизации помогает дополнительно снизить общие риски, однако при этом нужно учитывать такие факторы, как повышение стоимости и снижение производительности.

Классификация данных также может быть использована для определения политик решения различных других задач, связанных с управлением данными, включая:

- сроки хранения данных;
- политики доступа;
- требования к производительности для скоростей доступа и передачи;
- соответствие данных и управление рисками;
- предопределенное хранение данных;
- упрощение шифрования данных;
- индексирование данных;
- защиту данных.

Эффективные методы классификации данных основаны на оценке рисков, которая учитывает критические для качества и непрерывности обслуживания элементы. Оценка рисков используется для разработки политики внедрения, которая обеспечивает поддержку этих элементов для гарантии безопасного, эффективного и действенного использования данных.

У каждого предприятия или организации будет свой подход к классификации данных и политикам, применяемым к отобранным данным. Организации, желающие создать свою систему классификации данных, должны делать это осторожно и следовать передовым практикам.

Вопрос выбора данных для классификации и уровня классификации должен решаться политикой. Применяемая политика, как правило, определяется совокупностью факторов «Стоимость», «Риск» и «Заинтересованные стороны».

Стоимость относится к фактической стоимости информации для организации (ценными могут быть как данные о новом производственном процессе, так и финансовая информация), но кроме того, в стоимость могут быть включены потенциальные затраты на восстановление данных.

Риск, как правило, описывается сочетанием последствий события и вероятности их возникновения. Последствиями потери, утечки или повреждения данных могут быть потеря бизнеса, утрата репутации, а иногда даже уголовное или гражданское разбирательство.

Заинтересованные стороны — это те, кто заинтересован в безопасности данных, например другие отделы организации, значимые клиенты или государственные регулирующие органы.

Например, чтобы избегать рисков в соответствии с регламентами конфиденциальности, предприятие может решить, что все ПДн следует относить к классу среднего влияния на бизнес (MBI) или выше, а более чувствительные ПДн (например, медицинскую информацию) всегда следует относить к классу высокой степени воздействия на бизнес (HBI) или выше. Однако к этому же классу будет относиться и другая информация, которая вообще не содержит ПДн, например ценная финансовая информация или информация о конструкции. Помимо сказанного, для обработки данных, которые не отнесены к конкретному классу данных, как правило, имеется политика «по умолчанию».

С точки зрения управления данными процесс классификации ортогонален другим критериям, обсуждаемым в настоящем стандарте, включая процесс категоризации данных (см. 6.2.2). В случаях, когда данные подпадают как под политику управления данными, так и под политику классификации данных, как правило, применяется наиболее строгая политика. Таким образом, с практической точки зрения системы управления данными следует учитывать как политику, основанную на содержании (как описано в настоящем стандарте), так и политику на основе классификации, используемую в организации, и применять средства управления с учетом обоих аспектов с использованием соответствующих технических механизмов.

Выбор подходящей схемы классификации данных зависит от контекста приложения. Таким образом, настоящий стандарт не накладывает никаких ограничений на схему классификации данных, используемую в связи с таксономией данных. Требования к таксономии данных приведены в [1].

6.2.7 Дополнительные элементы, относящиеся к области приложения

Элементы структуры, описанные в 6.2.2—6.2.4, должны быть дополнены элементами, относящимися к выбранной области приложения. Например, политики безопасности данных могут быть определены в зависимости от общих целей безопасности, таких как конфиденциальность, целостность и доступность определенных категорий данных, с учетом классификации зависящих от приложения данных, как объяснено в 6.2.6. В некоторых случаях необходимо учитывать дополнительные специфичные для прикладной области аспекты. Например, политики, относящиеся к корпоративному управлению данными, могут быть представлены относительно жизненного цикла, определенного корпоративным управлением данными.

Настоящий стандарт не накладывает никаких ограничений на элементы, специфичные для области.

7 Использование структуры

7.1 Режимы использования структуры

Структуру обработки данных можно использовать:

- аналитически, чтобы понять, какие существующие правовые или организационные политики должны применяться при обработке определенного типа данных;
- для разработки политики обработки данных для определенных типов данных.

Как правило, необходимо использовать оба режима: аналитический режим обеспечивает условия, терминологию и ограничения для разработки политик обработки данных, которые должны быть реализованы техническими или организационными средствами.

7.2 Использование структурных элементов

7.2.1 Категории данных

Если категории данных (см. 6.2.2) используются для структурирования определения политик, то нет необходимости рассматривать все дерево категорий для всех приложений. Анализ или определение политики должны быть сосредоточены на тех категориях, которые для этого полезны:

- следует сосредоточиться только на выбранных категориях: например, для представления политики в отношении данных поставщика облачной службы можно игнорировать другие три категории верхнего уровня и все категории нижних уровней;
- если рассматриваемая политика может быть адекватно представлена в терминах категорий высшего уровня, категории нижнего уровня можно игнорировать;
- при необходимости допускается добавлять новые категории нижнего уровня к четырем категориям верхнего уровня (см. [1]).

7.2.2 Квалификаторы идентификации данных

По мере необходимости в представлении политики можно использовать квалификаторы идентификации данных, описанные в 6.2.3. Например, для информации, позволяющей установить личность, в зависимости от уровня обезличивания ПДн могут применяться различные политики обработки данных.

7.2.3 Области и действия

В [1] представлена детально проработанная концепция уровней, на которых определенное действие использует следующие данные:

- область источника: источник рассматриваемых данных;
- область использования: приложения или службы, использующие данные;
- область результата: набор измененных элементов в результате использования данных.

Эти понятия различных областей можно использовать непосредственно в политиках для представления требований и ограничений для источника данных, приложений или служб, которые используют эти данные, и результатов такой обработки данных. Перечень действий, описанный в 6.2.5, не является исчерпывающим и может быть расширен за счет дополнительных действий.

7.3 Представление политик

Настоящий стандарт не налагает никаких ограничений на способы представления политик. В частности, использование квалификаторов (см. 7.2.2), а также областей и действий (см. 7.2.3) не является обязательным. Эти элементы могут быть полезны для конкретных типов политик.

Самое простое представление политик может представлять собой единственную запись в таблице (например, «локально», «регионально» или «глобально» для описания политик, выражающих требования локализации для хранения и обработки данных). Но в то же время представление может быть сложным описанием мер и целей обеспечения безопасности и конфиденциальности, предусмотренных для определенного типа данных.

Структура спецификации использования данных (см. [1]), предоставляет средства для представления стандартизированным способом политик использования данных. Следовательно, для политик, которые ограничивают использование данных, или для политик определенной категории данных (с учетом объема или использования данных, действий по обработке данных и степени обезличивания данных, как описано в 6.2 и разделе 7), эта структура доступна как инструмент для представления и распространения политик обработки данных.

7.4 Пример

В таблице 1 приведен пример политики управления данными на основе общей структуры, предложенной в настоящем стандарте. Строки этой таблицы соответствуют категориям данных, а в колонках приведены общие аспекты управления размещением данных. Таким образом, пересечение каждой строки и колонки описывает конкретный выбор или настройку, выбранную для представления определенной политики управления данными для конкретного типа данных. Ячейки этой таблицы в совокупности описывают общую политику управления данными с точки зрения размещения.

Таблица 1 — Пример представления политики размещения данных

Категория данных		Размещение данных	
		Требование к размещению	Оператор
Данные контента клиента	Учетные данные	Локально	CSC
	Списки контента клиента	Локально	CSC
	Персональные медицинские данные	Локально	CSC
	Персональные данные детей	Локально	CSC
	Финансовые детали	Локально	CSC
Производные данные	EUII — данные телеметрии	Глобально	CSP
	EUII — история просмотров на стороне клиента	Локально	CSC
	EUII — социальные данные	Регионально	CSP, CSN
Данные поставщика облачной службы	Данные доступа и аутентификации	Глобально	CSP
	Операционные данные	Глобально	CSP
Данные учетной записи	Контактная информация клиента	Регионально	CSP
	Данные платежного инструмента	Глобально	CSP

Колонка «Размещение данных» в таблице 1 содержит набор примеров элементов, которые необходимо учитывать при определении политики размещения данных. Требование к размещению определяет, где должны храниться различные типы данных.

Настоящий стандарт не определяет одну или несколько политик данных, а предлагает общую структуру и основы, которые могут быть использованы для формирования оптимальной политики, результатом чего, как правило, будут структурированные, гармоничные представления политики.

8 Представление политик данных для конкретных проблемных областей

8.1 Общие положения

Практики и политики данных, рассматриваемые в этом разделе, являются типичными примерами основанных на категориях данных, необходимых для применения методов управления данными. Соответственно, каждое соображение является примером проблемы, которую необходимо учитывать при определении политики. Фактически политика управления данными определяется для каждой категории данных и каждой практики управления данными.

Рассматриваемые далее политики и методы управления данными относятся к наиболее распространенным практикам. Перечень рассмотренных политик и практик не является исчерпывающим и при необходимости может быть расширен дополнительными аспектами политик и практик.

8.2 Размещение данных

В качестве примера рассмотрим контролируемые глобально доступными облачными сервисами действующие политики или практики размещения данных.

Несмотря на большое число преимуществ инвестирования в развитие центров обработки данных, расположенных по всему миру, таких как сокращение задержки и обеспечение непрерывности обработки, поставщики облачной службы зачастую отдают предпочтение поддержке локальной обработки данных в соответствии с регламентами, политикой или предпочтениями размещения, связанными с вопросами обеспечения безопасности и защиты данных. Тем не менее для нескольких географически рассредоточенных центров обработки данных по-прежнему имеют место технические и инженерные ограничения. Данные ограничения усугубляются распределенной природой центров обработки данных. Облачные сервисы будут более рентабельными и надежными, если ими управлять централизованно как группой.

Таким образом, для обеспечения эффективного управления региональными и глобальными центрами обработки данных и услугами поставщики облачных служб должны четко и ясно определить, какие данные должны обрабатываться локально, а каким данным можно пересекать границы. Определить это может помочь общий и структурированный метод представления таких политик, позволяющий поставщику облачной службы точно определять размещение типов данных и их использование, а также определять несколько широких классов данных, которые далее будут использоваться в обсуждениях политики размещения и контрактов. Очевидно, что политики размещения данных являются хорошим примером тех типов политик данных, которым может быть полезен настоящий стандарт. Если такие политики выражены в общем и структурированном виде на основе общей таксономии данных, то стороны, заинтересованные в экосистеме облачных вычислений, смогут легче и эффективнее понимать, сравнивать и анализировать такие политики. Кроме того, общее и структурированное представление, сравнение и анализ таких политик и практик размещения лучше поддаются автоматизированному синтаксическому анализу и автоматизированной обработке, что обеспечивает простоту, точность и эффективность их обработки.

8.3 Трансграничная передача данных

8.3.1 Юрисдикция данных

8.3.1.1 Общие положения

Юрисдикция для облачных вычислений — это очень сложная предметная область, которая часто приводит к путанице. Для обработки данных, хранения данных и передачи данных имеются свои юридические аспекты. Для каждого из них есть конкретные политики, которые необходимо применять, основываясь на категоризации данных (как описано в [1]), необходимых уровнях классификации данных и применимых юрисдикциях.

В этом разделе представлена модель взаимодействия юрисдикции, основанная на понятиях «категоризация данных» и «классификация данных» (см. рисунок 5). Применяемые политики юрисдикции обозначены окружностями с заливкой для определения того, какие действия допустимы для данных. Системы категоризации данных могут различаться, а в [1] представлены лишь некоторые базовые элементы категоризации данных.

8.3.1.2 Географическая юрисдикция

Географическая юрисдикция может быть:

- муниципальной;
- региональной;
- национальной;
- международной.

Последняя представляет собой наиболее сложный тип географической юрисдикции различных форм и определяется двусторонними или многосторонними торговыми соглашениями и другими установленными действующими нормативными правовыми документами.

При развертывании облачной службы необходимо учитывать, что она может охватывать несколько географических юрисдикций.

Географические юрисдикции также могут иметь разные политики и регламенты, которые противоречат друг другу или частично совпадают, что усложняет взаимодействие как внутри юрисдикции, так и

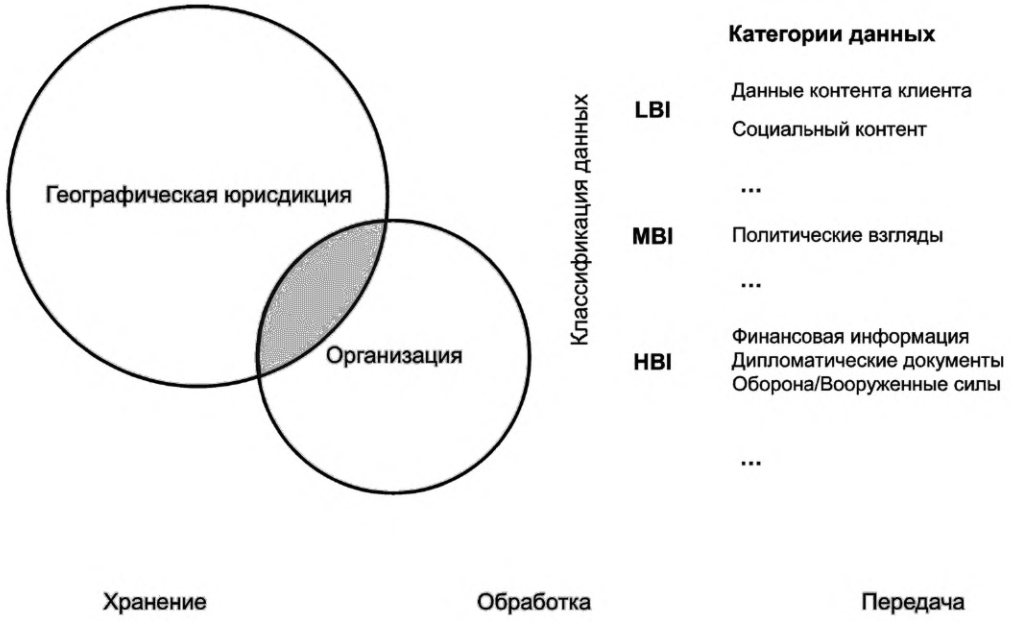

Рисунок 5 — Модель взаимодействий юрисдикций

между разными юрисдикциями. Например, федеральная политика по срокам хранения различных документов может отличаться от аналогичной политики на уровне региона или округа. Реальность такова, что такие противоречивости политик выявляются только сейчас в связи с тем, что облачные технологии и совместное использование процессов и данных показали, что такие политики не соблюдались в течение многих лет. Инициативы в области облачных вычислений предоставляют возможность выделять и стратегически решать эти проблемы. Чтобы политики соответствовали требованиям, их необходимо корректировать, возможно, временно/тактически.

Политики, основанные на географических юрисдикциях, различны.

Таблица 2 — Примеры политик на основе географической юрисдикции

Национальный уровень	Политики и регламенты обработки данных на федеральном/национальном уровне. Постановления правительства о данных. Регламенты обороны/вооруженных сил. Федеральные/национальные финансовые/банковские/инвестиционные регламенты. Федеральные/национальные регламенты электросвязи. Национальные регламенты по конфиденциальности. Национальные регламенты по медицинским записям. Национальные политики и регламенты по ПДн. Национальные регламенты правопорядка
Уровень региона/ округа	Политики и регламенты обработки данных на уровне региона/округа. Постановления правительства региона/округа о данных. Медицинские карты региона/округа. Политики и регламенты по ПДн на уровне региона/округа. Регламенты правопорядка региона/округа
Муниципальный уровень	Муниципальная политика по конфиденциальности данных
Международный уровень	Соглашения о свободной торговле и пр.

8.3.1.3 Предприятие/организация

Регламенты и политики предприятия распространяются:

- на политики данных для организации;

- записи сотрудников;
- записи клиентов;
- контракты и другие юридические документы;
- финансовые отчеты;
- интеллектуальную собственность.

Приведенный перечень не является исчерпывающим и может быть дополнен.

Организации могут использовать данную модель и специально определять соответствующие политики и конкретные интерпретации таким образом, чтобы развертывание облака могло осуществляться прозрачно и обеспечивало совместимость.

Вместе с географической юрисдикцией необходимо рассмотреть три основных базовых функции: хранение, обработку и передачу данных.

Большинство проблем, связанных с юрисдикцией для данных, связаны с конфиденциальностью и суверенитетом данных. ПДн обычно являются стимулирующим фактором, влияющим на политику и нормативные акты юрисдикции данных. В некоторых случаях политики юрисдикции данных поощряют хранение и обработку данных за пределами юрисдикции, в которой ведется бизнес. Например, в юрисдикциях, подверженных риску стихийных бедствий или политических беспорядков, данные лучше обрабатывать средствами облачных сервисов, размещенных за пределами их юрисдикции. Множество вариантов, целей и ограничений делают эту предметную область сложной, не имеющей единого решения.

Место хранения. Политики и регламенты размещения данных определяют, где данные не могут храниться. Проблемы зачастую связаны с конфиденциальностью данных и доступом к данным из-за юридических регламентов по раскрытию информации. Однако 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. [3]).

Обработка. Политика и регламенты обработки облачных вычислений определяют, где данные не могут обрабатываться. Обычно проблемы связаны с ограничениями производительности и доступности. Утечка данных изнутри процесса — еще один повод для беспокойства.

Передача. Политики и регламенты передачи (перемещения) данных облачных вычислений определяют, как данные могут перемещаться между сетевыми узлами поставщика и между клиентом и поставщиком. Часто опасения вызывают потенциальный перехват данных и/или ограничения производительности и доступности. Утечка данных во время передачи также является поводом для беспокойства.

8.3.2 Трансграничная передача данных

В современной экономике, в большой степени связанной с информацией, возможность легальной передачи данных из одной страны, региона, экономической или политической зоны в другую имеет решающее значение. При отправке или получении данных поставщиком и потребителем облачной службы действуют различные нормативные политики, а юрисдикции стран, в которых они базируются, влияют на требования к передаче данных.

Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с [3].

Поставщики облачной службы должны:

- убедиться, что данные клиентов, такие как данные, защищенные правами на результаты интеллектуальной деятельности или внутренние данные компании, достаточно защищены при перемещении из одной страны, региона, экономической или политической зоны в другую;
- убедиться, что ПДн в достаточной степени защищены, а в принимающих странах или зонах обеспечиваются права субъектов данных.

Основанный на таксономии подход (см. [1]) помогает поставщикам облачной службы:

- анализировать юридические или договорные требования к трансграничной передаче данных;
- обеспечивать клиентов информацией о режимах трансграничной передачи данных.

В общем случае передача данных из одной страны, региона, экономической или политической зоны в другую может базироваться на одном из следующих примеров политики или регулирования:

- договоры между передающей и принимающей сторонами, которые включают соответствующие меры обеспечения конфиденциальности и безопасности;
- согласие субъекта данных в случае передачи ПДн;

- обязательные корпоративные регламенты передачи данных между филиалами (или группами аффилированных лиц) корпорации;

- трансграничные регламенты: кодексы поведения, одобренные группами стран или зон, между которыми происходит передача данных;

- кодексы поведения, сертификаты и стандарты. Эти механизмы могут использоваться в различных вариантах реализации технических разъяснений и руководящих указаний по применению обязательных корпоративных или международных регламентов в отдельных секторах или отраслях;

- соглашения о «белых списках», основанных на достаточности. Эти договоренности об ответственности за передачу ПДн основаны на заключении об адекватности регламентов защиты данных в принимающей стране или регионе;

- исключения и отступления от ограничений на трансграничную передачу данных. Например, передача ПДн может быть разрешена в предусмотренных в [3] следующих случаях:

- наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

- предусмотренных международными договорами Российской Федерации;

- предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

- исполнения договора, стороной которого является субъект персональных данных;

- защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия субъекта персональных данных в письменной форме.

Учитывая этот набор механизмов, позволяющих на законных основаниях разрешать трансграничную передачу данных, поставщики облачной службы могут использовать категории данных для анализа их доступности и применимости, как показано в следующей таблице 3 для данных отправителей и получателей.

Таблица 3 — Гипотетический анализ доступных/применимых регламентов или политик для трансграничной передачи данных

<table>
<tr><th colspan="2" rowspan="2">Категории данных</th><th colspan="7">Нормативные акты</th></tr>
<tr><th>Договоры</th><th>Корпоративные регламенты</th><th>Трансграничные регламенты</th><th>Кодексы поведения</th><th>Белый список</th><th>Отступления/ исключения</th><th>Согласие</th></tr>
<tr><td colspan="2">Данные контента клиента</td><td rowspan="6">CSP/CSC должны проанализировать, достаточно ли контрактов для легальной трансграничной передачи данных</td><td colspan="4" rowspan="6">CSP/CSC должны проанализировать, какие механизмы доступны для легальной трансграничной передачи данных</td><td rowspan="6">CSP/CSC должны проанализировать, допускают ли юрисдикции в принимающих странах отступления или исключения</td><td rowspan="6">CSP/CSC должны запрашивать согласие субъектов данных, если другие инструменты неприменимы</td></tr>
<tr><td rowspan="2">Производные данные</td><td>EUII</td></tr>
<tr><td>OII</td></tr>
<tr><td rowspan="2">Данные CSP</td><td>Данные доступа и аутентификации</td></tr>
<tr><td>Операционные данные</td></tr>
<tr><td rowspan="2">Данные учетной записи</td><td>Контактная информация клиента</td></tr>
<tr><td>Данные платежного инструмента</td></tr>
</table>

8.4 Переносимость данных и доступ к данным

8.4.1 Общие положения

В этом разделе представлены основы того, как на основе категорий данных из общей таксономии данных с учетом связи хранимых данных с субъектом данных и с учетом политики обработки этих данных, выделить данные, которые должны удовлетворять требованиям переносимости данных с учетом конфиденциальности. Кроме того, здесь описываются методы формирования требований к передаче данных напрямую и методы работы с требованиями переносимости данных для тех из них, которые содержат персональные данные других субъектов данных, такие как социальные данные, опять же с учетом конфиденциальности.

Эти основы предлагают подход к предоставлению потребителю облачной службы возможностей при доступе к их контенту, подобных возможностям при передаче, с использованием аналогичных структур как для доступа к данным, так и для переносимости данных. Прямая передача принимающим операторам данных зачастую может обеспечиваться «моделью активного опроса», основанной на том, что принимающие операторы данных запрашивают и обрабатывают эти наборы данных по авторизованному запросу субъекта данных или потребителя облачной службы.

8.4.2 Информация, необходимая для переносимости или доступа к данным

На обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателей на рисунке 6 показано, какие типы данных в таксономии данных подпадают под требования переносимости данных или под требования политики или практики доступа к данным. В большинстве примеров политик данные контента клиентов рассматриваются с точки зрения требований к переносимости данных, за исключением лишь данных учетных записей.

Для производных данных и входящих в них подтипов данных могут потребоваться более детализированные политики. Например, для следующих категорий данных, относящихся к «телеметрии», переносимость данных или доступ к ним обычно не требуются:

- данные о работоспособности продуктов и услуг;
- данные о подключении и конфигурации устройства.

Эти две категории данных не связаны с субъектами данных, поскольку они относятся к производительности самой системы.

Такое структурированное и согласованное представление переносимости данных и доступа может стать основой определения того, когда требуется согласие пользователя. Это представление можно также использовать в кодексах поведения для выработки консенсуса по совокупности передовых практик в отрасли. Для кодексов поведения, связанных с переносимостью данных и доступом, наличие общих структур и согласованных формулировок политики способствует достижению и представлению консенсуса с предпочтительным уровнем точности.

Обработчики и операторы данных могут иметь различные политики и методы. Например, для переносимости данных или доступа к ним поставщики облачной службы, выступающие в качестве обработчиков данных, должны для поддержки своих потребителей облачной службы, действующих в качестве операторов, применять адаптированные методы. Поэтому, когда это применимо, каждое представление политики должно учитывать различные точки зрения оператора данных и обработчика данных.

В некоторых политиках степень зависимости от конкретного субъекта также может повлиять на требования переносимости данных или доступа к данным, когда квалификаторы идентификации данных в таксономии данных используются для представлений политики. Например, идентифицированные данные и псевдонимизированные данные могут быть связаны с субъектом данных, который, например, предоставляет соответствующий идентификатор. Следовательно, субъект данных может потребоваться для переносимости данных или доступа к ним, но он не требуется для переносимости данных или доступа к анонимизированным данным или данным, не связанным с субъектом данных. Однако несвязанные псевдонимизированные данные, вероятно, не могут потребоваться для переносимости данных или доступа к ним, в зависимости от предпочтительной действующей политики, поскольку эти данные не могут быть четко связаны с субъектом данных. Таким образом, в общем случае, если политика касается личных данных, то ее можно представить доступными в таксономии данных уровнями обезличивания.

8.4.3 Форматы и переносимость

Требования к совместимости и переносимости данных для облачных вычислений изложены в ГОСТ Р ИСО/МЭК 19941, который описывает основы переносимости данных и требования четких спецификаций синтаксиса и семантики данных, требуемых для успешной переносимости данных между двумя сторонами.

Категории данных			Требование переносимости	Идентифицированные данные	Псевдонимизированные данные	Несвязанные псевдонимизированные данные	Анонимизированные данные	Агрегированные данные
			Требуется переносимость данных	Да	Да	Нет	Нет	Нет
Данные контента клиента	Контент клиента — общее		Да	Да	Да	Да	Да	Да
	Списки контактов клиентов		Да	Да	Да	Да	Да	Да
	Персональные медицинские данные		Да	Да	Да	Да	Да	Да
	Учетные данные		Нет	Нет	Нет	Нет	Нет	Нет
Производные данные	EUII	Данные телеметрии	?	?	?	Нет	Нет	Нет
		Данные о подключении	?	?	?	Нет	Нет	Нет
		Наблюдаемое использование возможностей службы	Да	Да	Нет	Нет	Нет	Нет
		Демографическая информация	Да	Да	Нет	Нет	Нет	Нет
		Данные об интересах и предпочтениях	Да	Да	Нет	Нет	Нет	Нет
		Данные о потреблении контента	Да	Да	Нет	Нет	Нет	Нет
		История просмотров на стороне клиента	Да	Да	Нет	Нет	Нет	Нет
		Поисковые команды и запросы	Да	Да	Нет	Нет	Нет	Нет
		Местоположение пользователя	Да	Да	Нет	Нет	Нет	Нет
		Социальные данные	Да	Да	Нет	Нет	Нет	Нет
		Биометрические и медицинские данные	Да	Да	Нет	Нет	Нет	Нет
		Контактные данные конечного пользователя	Да	Да	Нет	Нет	Нет	Нет
		Данные о среде пользователя	Да	Да	Нет	Нет	Нет	Нет
Данные CSP	Данные об аутентификации и доступе		Нет	Нет	Нет	Нет	Нет	Нет

Примечания

1 В данном примере использованы следующие обозначения: «Да» — требуется переносимость данных; «Нет» — переносимость данных не требуется; «?» — не определено.

2 Предполагается, что данные контента клиента являются идентифицируемыми данными.

Рисунок 6 — Пример представления политики переносимости данных

Как показано в ГОСТ Р ИСО/МЭК 19941—2021 (пункт 5.2.2.6, таблица 2), пример синтаксической переносимости данных может поддерживаться популярными форматами, такими как XML или JSON, доступ к которым осуществляется посредством обмена файлами или через API. Однако для поддержки семантической переносимости требуется общее понимание определений, схем и структур, описанных в дополнительной документации и материалах для разработчиков. Переносимость данных между двумя разными системами всегда требует специальной обработки для сопоставления семантических различий и максимально возможного сохранения «метаданных». Особенно это важно для передачи производных данных, форма и содержание которых зависят от услуги.

В результате поддержка и представление переносимости данных политик для данных контента клиентов и для производных данных могут быть разными, отсюда и потребность в ориентированном на таксономию представлении таких политик или практик, определенных в этом разделе.

На рисунке 6 показан пример представления политики переносимости данных на основе категорий данных и квалификаторов обезличивания данных.

8.5 Использование данных

Что касается использования данных, структура, приведенная в разделе 6, определяет ряд вариантов обработки данных в зависимости от целей. На рисунке 7 показано, как эту структуру можно использовать для определения политик, связанных с конкретным использованием данных. Кроме того, области использования данных (см. 6.2.4) можно применять для дальнейшего уточнения определения соответствующих политик.

8.6 Управление данными

8.6.1 Безопасность данных

8.6.1.1 Общие положения

Для того чтобы учесть стратегическую важность данных, можно внедрить эффективную систему менеджмента информационной безопасности (СМИБ), как это описано в ГОСТ Р ИСО/МЭК 27001. СМИБ должна быть расширена таким образом, чтобы включить сторонние потоки данных и управление данными в сервисах облачных вычислений (см. ГОСТ Р ИСО/МЭК 27017). Данные стандарты содержат руководства по обеспечению информационной безопасности, но в некоторых случаях таких мер будет недостаточно, и руководящий орган должен будет полагаться на доверие и проверку.

Безопасность данных обычно определяют с точки зрения трех основных целей обеспечения безопасности, а именно конфиденциальности, целостности и доступности.

8.6.1.2 Цели обеспечения безопасности данных

Конфиденциальность определяется как недоступность для неавторизованных лиц, объектов или процессов (см. ГОСТ Р ИСО/МЭК 27000). Политика, обеспечивающая конфиденциальность, обычно определяет, кто (то есть какие объекты, такие как люди или системы) имеет доступ к данным и что ему разрешено с ними делать. Это часто обеспечивается с помощью технологий управления правами на доступ к данным (IRM) или управления цифровыми правами (DRM), сохраняя данные в зашифрованном виде, так что их можно использовать только при соблюдении всех требований политики. Если данные разрешено перемещать за пределы организации, то необходимо будет иметь гарантию, что на всем пути перемещения данным будет обеспечена соответствующая (или лучшая) защита.

Политика, связанная с конфиденциальностью, относительно редко непосредственно влияет на географические ограничения данных[1)]. Адресат гораздо важнее места назначения. Обычно для предотвращения проблем, связанных с утечкой данных или несанкционированным раскрытием, используются меры обеспечения безопасности, такие как обязательное использование надежного шифрования при хранении и передаче, при пересечении границ организации или особенно международных границ.

Пример — Документ, хранящийся в облаке, классифицируется и помечается как «Секрет компании», поскольку он содержит важную информацию о предстоящей позиции на переговорах. Применение географических ограничений нецелесообразно, поскольку это затруднит или сделает невозможным доступ к информации для переговорной группы во время их поездки на встречу. Однако компания использует IRM, чтобы гарантировать, что эта «конфиденциальная информация компании» будет доступна только уполномоченному лицу на защищенном устройстве с двухфакторной аутентификацией.

[1)] За исключением случаев лицензирования авторских прав с географическими ограничениями, когда сторонний контент, например медиаконтент или специализированные публикации, защищен географически ограниченной лицензией.

Категории данных			Действие						Область		
			Предоставлять	Улучшать	Персонализировать	Предлагать обновления/дополнительные возможности	Продавать/рекламировать/продвигать	Обмениваться	Первая сторона	Сторонние обработчики данных (партнеры)	Сторонние обработчики данных (прочие)
Данные контента клиента	Учетные данные		Да	N/A	N/A	N/A	N/A	Нет	Да	Да	Да
	Политические взгляды		A	Нет	A	A	A	A	Да	B	Нет
Производные данные	EUII	Данные телеметрии	Да	Да	Да	Да	Да	Да	Да	B	B
		Демографическая информация	Да	Да	Да	Да	Да	A	Да	B	B
		Местоположение пользователя	Да	Да	Да	Да	Да	A	Да	B	B
Данные CSP	Данные доступа и аутентификации		Да	Да	N/A	N/A	N/A	Нет	Да	B	Нет
	Операционные данные		Да	Да	Да	Да	Да	A	Да	Да	Да
Данные учетной записи	Контактная информация клиента		Да	Нет	N/A	Да	Да	A	Да	Да	C
	Данные платежного инструмента		Да	Да	N/A	N/A	N/A	Нет	Да	Да	Да

Примечание — В данном примере использованы следующие обозначения:

«Да» — использование возможно в соответствии с обычной политикой, например политикой безопасности данных;

«Нет» — использование данных невозможно;

A — в зависимости от правил защиты конфиденциальности, от разрешений;

B — в зависимости от договоров, контрактов, разрешений;

C — в зависимости от контрактов;

N/A — использование категории данных невозможно.

Рисунок 7 — Пример представления использования данных

Целостность данных — это свойство сохранения правильности и полноты активов (см. ГОСТ Р ИСО/МЭК 27000). Политики, связанные с целостностью данных, часто требуют, чтобы

данные, к которым применяется политика, имели более высокую гарантию целостности, чем обычные данные. Это означает, что данные поддерживаются в правильном состоянии и могут быть изменены только преднамеренными и санкционированными способами. Следовательно, необходимо обеспечить обнаружение и устранение всех случайных ошибок, возникающих из-за неисправностей носителя данных или других случайных событий. Например, можно поддерживать несколько копий данных, каждой с контрольными суммами или другими проверками целостности, так что «плохая» копия может быть заменена заведомо исправными данными. Ошибки, вызванные действиями человека, можно идентифицировать и исправить. Как правило, это осуществляется посредством отслеживания изменений, журналов регистрации событий, свежих распределенных реестров и, возможно, иных экспертных подходов к анализу.

Пример — База данных, хранящаяся в облаке, содержит записи студентов, включая результаты тестов и выданные сертификаты. Хотя данные не являются строго конфиденциальными (не покрываются защитой ПДн), очень важно, чтобы они были защищены от несанкционированного изменения. Записи «заблокированы», чтобы предотвратить редактирование, периодически создается постоянная автономная копия, используемая для идентификации каких-либо изменений, которые могли быть внесены.

Доступность — это свойство, определяющее возможность использования объекта авторизованным субъектом по запросу (см. ГОСТ Р ИСО/МЭК 27000). Политики, связанные с доступностью, часто требуют, чтобы доступность для легальных пользователей важных данных была бы выше, чем обычных данных. Эффективная работа бизнеса требует, чтобы необходимые для работы данные были доступны в любой момент. Следовательно, необходимо уделить внимание дополнительным методам доступа к данным, таким как географическая избыточность и предоставление альтернативных сетевых путей.

Категории данных			Пункт политики								
			Конфиденциальность			Целостность			Доступность		
			HBI	MBI	LBI	HBI	MBI	LBI	HBI	MBI	LBI
Данные контента клиента	Учетные данные		X			X				X	
	Списки контактов с клиентами		X			X				X	
	Финансовые детали		X				X				X
Производные данные	EUII	Данные телеметрии	I,P	UP	A, AG		X				X
		История просмотров на стороне клиента	I,P	UP	A, AG		X				X
		Социальные данные	I,P	UP	A, AG	X					X
Данные CSP	Данные доступа и аутентификации		X			X			X		
	Операционные данные			X			X		X		
Данные учетной записи	Контактная информация клиента			X			X		X		
	Данные платежного инструмента		X			X			X		

Примечание — В данном примере использованы следующие обозначения:
I — идентифицируемые данные;
P — псевдонимизированные данные;
UP — несвязанные псевдонимизированные данные;
A — анонимизированные данные;
AG — агрегированные данные;
X — политики, которые надо определить для класса влияния (HBI, MBI или LBI).

Рисунок 8 — Пример использования таксономии данных для определения политик безопасности

8.6.1.3 Структура управления безопасностью данных

На рисунке 8 показано, как категоризацию данных можно применить для определения требований к политикам безопасности для данной организации. Общая классификация данных по влиянию: высокое/среднее/низкое влияние на бизнес используется для каждой из основных целей безопасности.

Например, учетные данные, списки контактов клиентов и финансовые данные определены как имеющие большое влияние на бизнес в случаях нарушения требований конфиденциальности. Нарушение требований целостности финансовых данных имеет средний эффект только потому, что во многих случаях можно восстановить эти данные из других источников и предполагается, что организация, выполняющая анализ проблемы, имеет доступ к этим источникам.

Записи для производных данных дополнительно иллюстрируют, как квалификаторы идентификации данных могут использоваться для определения требований безопасности: нарушения конфиденциальности для идентифицированных или псевдонимизированных данных имеют большее влияние на бизнес, чем для несвязанных псевдонимизированных или анонимизированных и агрегированных данных.

8.6.2 Качество данных

8.6.2.1 Общие положения

Качество данных означает точность, достоверность, надежность, своевременность, актуальность и полноту данных, используемых для конкретной цели. Управление качеством данных включает в себя политики, обязанности и процессы для сбора, обслуживания, хранения и передачи данных. Управление качеством данных связано с рассмотренными далее аспектами.

8.6.2.2 Задачи управления данными

а) Очистка данных

Под очисткой данных понимается процесс проверки и исправления данных для обеспечения их соответствия стандартизированному формату (см. ГОСТ Р ИСО 13008). Он включает в себя анализ качества данных в источнике данных, определение мер и предложений о том, как можно улучшить качество данных, и внесение изменений в данные.

б) Управление метаданными

Управление метаданными может быть определено как сквозной процесс и структура управления для создания, контроля, улучшения, атрибуции, определения и управления схемой, моделью или другой структурированной системой агрегирования метаданных, независимо или в пределах репозитория и связанных поддерживающих процессов, как правило, для управления контентом.

в) Целостность данных

Целостность данных как цель безопасности уже обсуждалась в 8.6.1.2, но ее также можно рассматривать и с точки зрения управления качеством данных.

г) Обеспечение качества данных

Обеспечение качества данных означает уверенность в управлении качеством данных, которое может быть проверено посредством процедур сертификации и аудита.

д) Происхождение данных

Под происхождением данных (Data provenance) понимается запись изменения состояния данных в течение их срока службы, времени возникновения, лиц, связанных с событием, местоположения, программного обеспечения, причин, по которым событие произошло. Для поддержки происхождения данных могут использоваться механизмы, обеспечивающие неизменное свидетельство модификации, передачи и использования данных, такие как технологии распределенного реестра и блокчейна.

8.6.2.3 Структура управления качеством данных

Достижение приемлемого уровня управления качеством данных во многом зависит от рассматриваемого варианта использования. Проблемы с качеством данных могут не иметь значения для многих типов приложений, однако могут повлиять на другие приложения, критические для непрерывности бизнеса. К тому же обязанности по управлению данными могут быть по-разному распределены между поставщиком и потребителем облачной службы. На рисунке 9 показан пример того, как таксономия данных структуры может быть использована для определения ответственности за управление качеством данных.

8.7 Корпоративное управление данными

Данные — это нерасходуемый актив со многими связанными атрибутами и аспектами. Они должны рассматриваться руководящим органом организации как элементы, которые могут иметь существенное стратегическое влияние на организацию в целом. Данные используются для отслеживания бизнеса (например, персонала, бухгалтерского учета, запасов) и в качестве исходного материала для знаний, инноваций и понимания. Ответственность за данные и их использование возлагается на руководящий орган организации. Некоторые данные, такие как исследования продуктов или нераскрытые амбиции фондового рынка, имеют высокую ценность для бизнеса, и для использования и защиты этих данных необходимо задействовать соответствующие ресурсы. Стоимость и риск, связанные с управлением этими данными, выше, чем у других типов данных, и стратегии и политики должны отражать это посредством принятия схемы классификации данных. Руководящий орган несет ответственность за данные и их использование, включая решения по обеспечению надлежащего уровня управления данными.

В [4] описано применение общих принципов корпоративного управления ИТ и модели ГОСТ Р ИСО/МЭК 38500 к корпоративному управлению данными. В нем исследуются области использования организацией данных, в которых должны быть внедрены политики и стратегии корпоративного управления для обеспечения подотчетности. Исследование включает в себя понимание потенциального использования данных (организацией, ее поставщиками и клиентами, а также ее конкурентами), включая возможную покупку или продажу данных. Например, производитель может включить в свой продукт возможности, которые позволяют передавать данные об использовании продукта производителю. Эти данные могут быть использованы для улучшения продукта, оказания технической поддержки или профилактического обслуживания. Их также можно использовать в качестве основы при расчете оплаты использования продукта, а не прямой покупки. Данные также могут быть проданы производителем другим производителям для использования их при создании продуктов или услуг или переданы поставщикам для улучшения общей цепочки поставок. Кроме того, данные об использовании могут быть объединены с дополнительными данными, такими как погода, чтобы лучше понять использование продукта в различных условиях. Сами данные становятся частью цепочки создания стоимости.

Поскольку данные имеют стоимость, они также несут в себе риск для организации. Кроме того, могут быть ограничения на использование данных, налагаемые законами, нормативными актами, нормами общества или самой организацией.

Категории данных	Очистка данных	Управление метаданными	Обеспечение целостности	Гарантия качества	Происхождение данных
Данные контента клиента	CSC: в зависимости от варианта использования	CSC: в зависимости от варианта использования	CSC: в зависимости от варианта использования	CSC: в зависимости от варианта использования	CSC: в зависимости от варианта использования
Производные данные	CSP: политики операций и аудита	CSP: политики операций, безопасности и аудита	CSP: политики операций, безопасности и аудита	CSP: аудит	CSP: процесс, технические меры (например, блокчейн)
Данные CSP	CSP: операции и безопасность	CSP: операции и безопасность	CSP: операции и безопасность	CSP: аудит	CSP: в зависимости от варианта использования
Данные учетной записи	CSP: обязательный	CSP: обязательный	CSP: обязательный	CSP: аудит	CSP: процесс, технические меры (например, блокчейн)

Рисунок 9 — Пример использования таксономии данных для получения политик качества данных

В [4] представлено руководство по созданию исчерпывающего контрольного списка рекомендаций для руководящего органа при разработке структуры корпоративного управления данными для данной организации. Этот контрольный список обеспечивает максимальное использование данных в рамках организации с учетом уровня приемлемых рисков, а также внешних и внутренних ограничений.

Таким образом, структура корпоративного управления данными определяет стратегию данных, которая в свою очередь поддерживает и влияет на общую политику организации.

Необходимо определить общую стратегию данных и поддерживающую структуру руководства с учетом [5], в котором приведено «то, что руководящий орган организации ожидает и требует от группы по управлению данными, чтобы быть уверенным в том, что руководящие принципы ИТ могут быть реализованы и соблюдаются в отношении данных и их использования организацией». Механизм достижения этой гарантии заключается в том, что группа управления данными должна работать с руководящим органом для разработки политик управления данными, согласования и поддержки стратегии данных, как показано на рисунке 10.

Политики данных, реализованные группой управления данными, должны применяться ко всей совокупности данных, используемых организацией, включая данные, которые покупаются, продаются, передаются, обрабатываются, хранятся и т. д. Политики данных должны быть согласованы с другими связанными с данными политиками и практиками, описанными в настоящем стандарте, таким образом часть приведенной выше диаграммы может быть расширена для того, чтобы охватить спецификации использования данных, как показано на рисунке 11.

У поставщика облачной службы есть организационная цель и стратегии достижения этой цели, из которых можно получить стратегию данных, а также политики, поддерживающие использование данных. Спецификации использования данных могут быть созданы с учетом этих политик. Такие спецификации использования будут согласованы с общими бизнес-целями поставщика облачной службы.

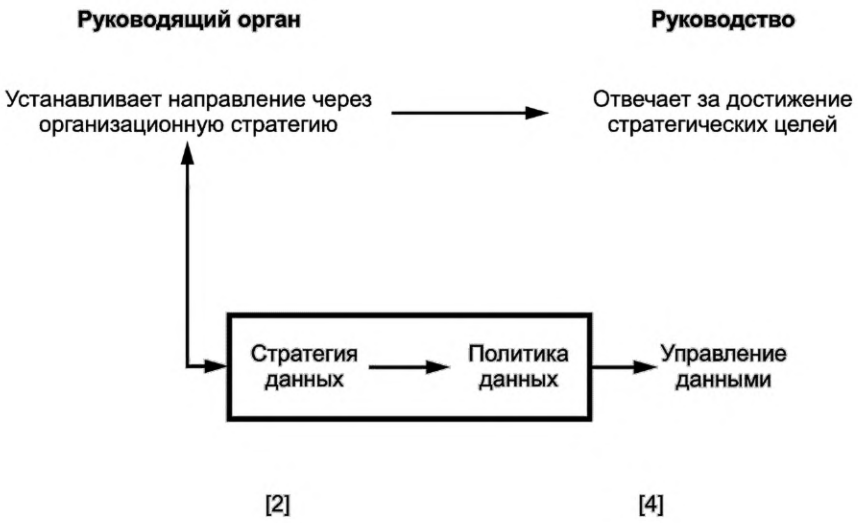

Рисунок 10 — Стратегия и политика данных (см. [5])

Рисунок 11 — Согласование стратегии данных, политик и спецификаций использования данных

Подобным образом потребитель облачной службы может описать стратегию обработки данных, которая поможет ему достичь целей своей организации. Как минимум, потребитель облачной службы должен гарантировать, что спецификации использования данных, предоставленные поставщиком облачной службы, соответствуют их собственным политикам данных, а также их собственным спецификациям использования данных в случаях, если они имеются.

Например, организационные цели поставщика по предоставлению облачной услуги облачной службы предусматривают предоставление услуги, которая:

- легко доступна из любого места;
- обеспечивает практически неограниченные масштабируемость, производительность, безопасность и надежность корпоративного уровня;
- соответствует местным нормам и требованиям.

Такие цели являются целями очень высокого уровня, и для их достижения требуется более детальное изучение. В таблицах 4—6 это рассмотрено с точки зрения поставщика облачной службы, и результирующие политики, полученные обобщением ячеек каждой строки, являются политиками поставщика облачной службы. Потребителю облачной службы следует изучить эти политики, чтобы убедиться, что они соответствуют их собственным политикам и надлежащему использованию данных для своей организации.

Кроме того, эти высокоуровневые политики корпоративного управления служат основой для других политик управления данными поставщика облачной службы, рассмотренных в настоящем стандарте. Политики должны быть четко согласованы, так чтобы управление данными осуществлялось в соответствии с политиками уровня корпоративного управления и способствовало организации в достижении ее целей.

Таблица 4 — Пример рабочего листа политики корпоративного управления данными (с точки зрения поставщика облачной службы)

Аспекты корпоративного управления данными	Руководство политиками данных			
	Значимость	Риск	Ограничения	Возможные политики
Сбор	CSC может собирать все виды данных со всего мира. Сбор статистики использования и другой телеметрии. Отраслевые данные, включая использование энергии, социальную ответственность и сертификаты, для обеспечения лидирующих позиций. Для выставления счетов требуется использование CSC. ПДн необходимы физическим лицам для доступа к некоторым услугам	Ценные данные могут стать причиной постоянных кибератак. Собранные данные могут быть использованы в незаконных целях	Данные о состоянии здоровья и ПДн могут потребовать специальной обработки. CSP будет обрабатывать данные от имени CSC	Стратегия CSP заключается в предоставлении услуг, позволяющих простую регистрацию клиентов и получение данных. CSC разрешает CSP обработку данных
Хранение	Необходимо повысить производительность и сэкономить за счет хранения данных в соответствии с частотой доступа. Необходимо уменьшить задержку за счет хранения данных вблизи обработки. Необходимо повысить надежность за счет репликации	Стихийные бедствия. Риски кибербезопасности, включая вредоносное ПО, полученное от CSC	Данные могут храниться внутри страны	Центры обработки данных должны физически располагаться в 10 регионах с наибольшим объемом рынка облачных вычислений. Данные должны быть недоступны для CSP, за исключением отдельных случаев доступа правоохранительных органов
Отчет	Данные телеметрии необходимы для улучшения услуг, включая стратегическое расширение или изменение услуг, персонала и центров обработки данных. Системы расчета требуют оценки использования CSC. Данные могут быть использованы для мониторинга инцидентов безопасности	Качество показателей может быть нестабильным. Действия по оценке влияют на производительность системы	Данные телеметрии не должны раскрывать ПДн	Действия по оценке CSP не должны превышать 0,05 % от общей производительности, а влияние этих действий CSC должно быть не заметно для CSC

Окончание таблицы 4

Аспекты корпоративного управления данными	Руководство политиками данных			
	Значимость	Риск	Ограничения	Возможные политики
Решение	Необходимо использовать инструменты анализа и ИИ для данных телеметрии, чтобы улучшить, расширить или сократить услуги. Анализ безопасности услуг — для защиты CSC, а также операций CSP	Нужно убедиться в правильности сбора данных для решений	Нет	CSC должны быть защищены как от внешних атак, так и друг от друга
Распространение	Некоторая телеметрия поставщикам (управление производительностью, проектные данные, оценки надежности и т. д.)	Управление доступом к данным. Данные телеметрии и биллинга могут быть строго конфиденциальными для CSP и CSC	Ограничение данных контента CSC правоохранительным органам при наличии действительного запроса и CSC, где это возможно	Данные телеметрии, использования и выставления счетов следует относить к категории конфиденциальных и ценных
Удаление	CSC должен управлять удалением своих данных	Необходимо определить возможность восстановления данных	Надлежащее удаление данных, собранных организациями и государством, в соответствии с требованиями соответствующей юрисдикции	Убедитесь, что все хранимые данные зашифрованы, чтобы оборудование можно было утилизировать без очистки

После создания таких политик данных уровня корпоративного управления поставщик облачной службы может исследовать определенные категории данных на основе таких аспектов управления данными, как сбор, хранение и составление отчетов.

Помимо прочего, полученная в результате политика представляет собой совокупность требований таблицы. Политики такого уровня могут быть включены в соглашения с потребителями облачной службы, а также детализированы в спецификациях использования данных.

Таблица 5 — Пример рабочего листа политик конкретных категорий данных: сбор (с точки зрения поставщика облачной службы)

Категории данных	Корпоративное управление политикой данных			
	Значимость	Риск	Ограничения	Политика
Данные контента клиента	Неприменимо	Неприменимо	Неприменимо	CSC определяет, какие данные собирать
Производные данные	Неприменимо	Неприменимо	Неприменимо	Неприменимо
Данные CSP	Неприменимо	Неприменимо	Неприменимо	Неприменимо
Данные учетной записи	Показатели дохода	Неприменимо	Неприменимо	Данные учетной записи считаются ценными данными

Таблица 6 — Пример рабочего листа политик для конкретных категорий данных: хранение (с точки зрения поставщика облачной службы)

Категории данных	Корпоративное управление политикой данных			
	Значимость	Риск	Ограничения	Политика
Данные контента клиента	Данные контента CSC являются косвенным источником дохода CSP, поскольку требуют использования услуг CSP	—	Любые данные CSC, используемые для исследований службы поддержки, должны быть уничтожены по завершении расследования службы поддержки	CSC несет ответственность за содержание хранимых данных. CSC гарантирует CSP отсутствие хранения незаконных данных (например, специальных ПДн, данных о состоянии здоровья, незаконных изображений). Данные CSC не будут использоваться для рекламы. CSC сохраняет все права на данные CSC
Производные данные	Косвенный доход от использования услуг. Поведение для прогнозирования сигналов безопасности. Телеметрия для улучшения услуг	Недопустима утечка идентифицируемых данных CSC в производные данные	Неприменимо	Неприменимо
Данные CSP	Неприменимо	Неприменимо	Неприменимо	Неприменимо
Данные учетной записи	Показатели дохода	Неприменимо	Неприменимо	Неприменимо

9 Применение структуры к кодексам поведения

Кодексы поведения отражают согласованные отраслевые или нормативные предпочтительные или требуемые политики или практики. Настоящий стандарт может быть полезен при представлении такой согласованной политики или практики, связанной с данными. Документированное согласие, зафиксированное в кодексах поведения, часто требует однозначных и точных формулировок обработки и использования данных с необходимым уровнем подробностей и детализации. Если подобные политика и практика связаны с данными, то, как правило, их нужно выразить в терминах таксономии данных с использованием методов и приемов, описанных в настоящем стандарте.

Вот несколько примеров использования кодексов поведения:

- кодексы поведения для промышленного сектора в регионе или стране, в экономической или политической зоне или для группы стран, связанных между собой договором или иным многосторонним соглашением, регламентирующие практики и политики, ориентированные на данные для этого промышленного сектора (например, здравоохранение, финансы, производство, энергетика). Такие кодексы поведения могут требоваться по закону или создаваться добровольно на основе отраслевого консенсуса;
- кодексы поведения для нормативной или государственной политики в стране, в экономической или политической зоне или для группы стран, связанных международными соглашениями (например, кодексы поведения, созданные для соблюдения одного или нескольких разделов общего регламента защиты персональных данных). В таких случаях кодексы поведения могут быть созданы одним или несколькими правительствами или заинтересованными сторонами отрасли, которые подпадают под действие этих нормативных или государственных политик;
- кодексы поведения, внутренние по отношению к организации, работающей в стране, или международной организации, регламентирующие методы и политику, ориентированные на данные, внутри этой организации.

В качестве примера рассмотрим поток данных через геополитические границы. На рисунке 12 приведен пример того, как структуры, касающиеся размещения данных, трансграничного потока данных, а также переносимости данных, определенные в настоящем стандарте, могут использоваться в кодексах поведения, направленных на поток данных и переносимость данных в экономической зоне или в пределах общего рынка.

Категории данных			Идентифицированные данные	Псевдонимизированные данные	Несвязанные псевдонимизированные данные	Анонимизированные данные	Агрегированные данные
Данные контента клиента	Общий контент клиента		1	1	3	3	4
	Списки контактов клиентов		1	1	3	3	4
	Персональные медицинские данные		1	1	2	3	4
	Учетные данные		1	N/A	N/A	N/A	N/A
Производные данные	Информация, позволяющая идентифицировать конечного пользователя	Общие производные данные	1	1	3	4	4
		Данные телеметрии	1	1	3	4	4
		Данные о подключении	1	1	3	4	4
		Наблюдаемое использование возможностей обслуживания	2	2	3	4	4
		Демографическая информация	2	2	3	4	4
		Данные об интересах и предпочтениях	1	1	3	4	4
		Данные об использовании контента	2	2	3	4	4
		История просмотров на стороне клиента	2	2	3	4	4
		Поисковые команды и запросы	2	2	3	4	4
		Местоположение пользователя	1	1	3	4	4
		Социальные данные	1	1	3	4	4
		Биометрические и медицинские данные	1	1	3	4	4
		Контактные данные конечного пользователя	1	1	2	3	3
		Данные о среде пользователя	2	2	3	4	4
Данные CSP	Общие данные CSP		4	4	4	4	4
	Данные об аутентификации и доступе		3	3	4	4	4
	Операционные данные		4	4	4	4	4

Примечание — Необходим обмен данными между поставщиками, потребителями облачной службы и партнерами по облачным сервисам:

1 — только внутри страны;

2 — только в пределах экономической или политической зоны;

3 — вне пределов экономической или политической зоны;

4 — глобально;

N/A — неприменимо.

Рисунок 12 — Пример кодексов поведения на основе таксономии данных — свободная передача данных в пределах экономической зоны или общего рынка

На рисунке 13 пример соглашения в части кодексов поведения для требований переносимости данных на основе таксономии данных в пределах экономической зоны или общего рынка.

Категории данных			Идентифицированные данные	Псевдонимизированные данные	Несвязанные псевдонимизированные данные	Анонимизированные данные	Агрегированные данные
Данные контента клиента	Общий контент клиента		2	2	3	4	4
	Списки контактов клиентов		2	2	3	4	4
	Персональные медицинские данные		2	2	3	4	4
	Учетные данные		Нет	Нет	Нет	Нет	Нет
Производные данные	Информация, позволяющая идентифицировать конечного пользователя	Общие производные данные	Нет	Нет	Нет	Нет	Нет
		Данные телеметрии	Нет	Нет	Нет	Нет	Нет
		Данные о подключении	Нет	Нет	Нет	Нет	Нет
		Наблюдаемое использование возможностей обслуживания	1	1	Нет	Нет	Нет
		Демографическая информация	1	1	Нет	Нет	Нет
		Данные об интересах и предпочтениях	1	1	Нет	Нет	Нет
		Данные о потреблении контента	1	1	Нет	Нет	Нет
		История просмотров на стороне клиента	1	1	Нет	Нет	Нет
		Поисковые команды и запросы	1	1	Нет	Нет	Нет
		Местоположение пользователя	1	1	Нет	Нет	Нет
		Социальные данные	1	1	Нет	Нет	Нет
		Биометрические и медицинские данные	1	1	Нет	Нет	Нет
		Контактные данные конечного пользователя	1	1	Нет	Нет	Нет
		Данные о среде пользователя	1	1	Нет	Нет	Нет
Данные CSP	Общие данные CSP		Нет	Нет	Нет	Нет	Нет
	Данные об аутентификации и доступе		Нет	Нет	Нет	Нет	Нет
	Операционные данные		Нет	Нет	Нет	Нет	Нет

Примечание — Необходим обмен данными между поставщиками, потребителями облачной службы и партнерами по облачным сервисам:

1 — только внутри страны;

2 — только в пределах экономической или политической зоны;

3 — вне пределов экономической или политической зоны;

4 — глобально;

N/A — неприменимо;

«Нет» — переносимость данных не требуется.

Рисунок 13 — Пример кодексов поведения на основе таксономии данных — переносимость данных в пределах экономической зоны или общего рынка

Приведенные выше примеры демонстрируют, как кодексы поведения, ориентированные на данные, могут быть представлены с предпочтительным уровнем точности и детализации. Более того, представление политики и практики в данных кодексах поведения более эффективно, если они выражаются на основе категорий и уровней обезличивания задействованных данных.

Таблица 7 представляет собой пример соглашения в части кодексов поведения на основе таксономии данных, которые касаются переносимости данных для облачных служб типа возможностей приложений (например, службы SaaS). Этот пример основан на переносимости облачных данных и трех аспектах: синтаксическом, семантическом и политическом, как это описано в разделе 8 ГОСТ Р ИСО/МЭК 19941—2021. Кроме того, этот стандарт описывает эти аспекты на основе одного из трех типов облачных услуг: приложений, платформ и инфраструктуры.

Таблица 7 — Пример кодексов поведения на основе таксономии данных: переносимость данных для облачных сервисов типа приложений

Категории данных			Синтаксис данных	Семантика данных	Политика данных
Данные контента клиента	Общий контент клиента		JSON	Comm	Локальность данных, безопасность, конфиденциальность
	Списки контактов клиентов		OOXML	Comm	Локальность данных, безопасность, конфиденциальность
	Персональные медицинские данные		Custom1	H	Локальность данных, безопасность, конфиденциальность, здоровье
	Учетные данные		ASCII	N/A	Локальность данных, безопасность
Производные данные	Информация, позволяющая идентифицировать конечного пользователя	Общие производные данные	N/A	N/A	N/A
		Данные телеметрии	JSON	Comm	Локальность данных, безопасность, конфиденциальность, права доступа
		Данные о подключении	JSON	Comm	Безопасность
		Данные об использовании возможностей обслуживания	CSV	Photo	Безопасность, конфиденциальность, совместное использование
		Демографическая информация	ASCII	SM	Безопасность, конфиденциальность, совместное использование
		Данные об интересах и предпочтениях	JSON	SM	Безопасность, конфиденциальность, совместное использование
		Данные о потреблении контента	JSON	Photo	Безопасность, конфиденциальность, совместное использование
		История просмотров на стороне клиента	CSV	SM	Безопасность, конфиденциальность, совместное использование

Окончание таблицы 7

Категории данных			Синтаксис данных	Семантика данных	Политика данных
Производные данные	Информация, позволяющая идентифицировать конечного пользователя	Поисковые команды и запросы	CSV	Hu	Безопасность, конфиденциальность, совместное использование
		Местоположение пользователя	Custom2	Comm	Безопасность, конфиденциальность, совместное использование данных, локальность данных
		Социальные данные	JSON	SM	Безопасность, конфиденциальность, совместное использование
		Биометрические и медицинские данные	Custom3	H	Безопасность, конфиденциальность, совместное использование данных, локальность данных, здоровье
		Контактные данные конечного пользователя	ASCII	Общий	Безопасность, конфиденциальность, совместное использование
		Данные о среде пользователя	JSON	Comm	Безопасность, конфиденциальность, совместное использование
Данные CSP	Общие данные CSP		Переносимость не требуется	Переносимость не требуется	Переносимость не требуется
	Данные об аутентификации и доступе		Переносимость не требуется	Переносимость не требуется	Переносимость не требуется
	Операционные данные		Переносимость не требуется	Переносимость не требуется	Переносимость не требуется

Таблица 8 — Пояснение к таблице 7: ключевые обозначения, описывающие переносимость данных

Синтаксис	Семантика		Политика (регулирующая или корпоративная)
ASCII, JSON, CSV, XML, OOXML, Custom1, Custom 2	Модели предметной области: коммуникации (Comm), фотография (Photo), человеческие ресурсы (Hu), социальные сети (SM), здравоохранение (H), музыка (M) и т. д.	Используемые семантические языки: OWL, Resource Description Framework (RDF), нотации моделирования, такие как UML и язык управления бизнес-процессами (BPML), — это инструменты, которые можно использовать для документирования и обмена знаниями	Локальность данных, права доступа, использование данных, совместное использование данных, безопасность, конфиденциальность, регламенты здравоохранения (здоровье)

В таблице 7 для каждого аспекта переносимости данных выбрано несколько вариантов и возможностей из доступных вариантов посредством ключевых обозначений. Например, синтаксическая переносимость данных контента клиента обеспечивается синтаксисом JSON, а учетные данные передаются в простом формате ASCII. Для семантической переносимости данных пример указывает на то, что данные контента клиента предполагают семантические определения для коммуникации приложений, но не из области фотографии или человеческих ресурсов. Аналогично данные контента клиента регулируются политиками в отношении локальности данных, безопасности и конфиденциальности. Однако для переносимости персональных данных о здоровье необходимо также учитывать применимые в этой юрисдикции регламенты здравоохранения.

Приложение А
(справочное)

Пример использования настоящего стандарта

А.1 Описание

А.1.1 Сценарий

Гипотетический поставщик облачной службы использует элементы структуры, описанные в разделе 6, для анализа требований к своим политикам использования данных и для формирования спецификаций конфиденциальности данных для потребителей облачной службы и пользователей облачных служб. Поставщик облачной службы описывает свои политики использования данных следующими вопросами:

- требование согласия пользователя: требуется ли явное согласие пользователя (дополнительно) или использование данных основано на законных правах поставщика облачной службы?
- требование уведомления: требуется ли явное (заметное) уведомление об использовании данных или достаточно того, что указано в спецификации конфиденциальности?
- дополнительные средства контроля: требуются ли дополнительные средства контроля клиентов, которые позволяют разрешать/запрещать ему использование определенных данных?

В таблице А.1 эти вопросы обобщены и представлены коды, используемые для обозначения политик использования данных в последующем анализе.

Таблица А.1 — Коды для политик использования данных

Политика в отношении	Коды	
Уведомление	P — заметное/явное	D — видимое
Согласие	N — согласие не требуется	O — требуется явное согласие
Контроль клиентов	A — необходим	B — не требуется
	X — не допускается или неприменимо	

Например, код P-O-B указывает на то, что требуется явное уведомление, для использования данных требуется явное согласие, а контроль клиентов не требуется.

Примечание — Следующее определение политик и спецификаций использования производных данных является чисто гипотетическим. Какой-либо связи с какими-либо существующими регламентами нет. В реальности для определения политик следует руководствоваться соответствующими нормативными и законодательными документами.

А.1.2 Мотивы

Пример использования демонстрирует:

- как использовать структуру (см. [1]) для определения сложных организационных политик с использованием табличного формата в качестве основы для анализа, и как получить спецификацию использования данных;
- влияние квалификаторов идентификации данных на сложность и применимость политик, связанных с конфиденциальными данными, такими как данные, позволяющие установить личность или организацию:
- политики для идентифицированных данных, как правило, более сложны, чем политики для обезличенных данных. Политики для анонимизированных или агрегированных данных наиболее просты;
- интенсивность использования данных уменьшается с увеличением степени обезличивания. В то время, когда идентифицируемые данные могут использоваться для самых разных целей, использование анонимизированных или агрегированных данных довольно ограничено.

Не все комбинации элементов структуры, таких например, как действия и области действия, значимы. То, какие комбинации применяются, зависит от приложения. Выбор набора значимых комбинаций может значительно упростить процесс определения политики.

А.2 Спецификации анализа и использования производных данных

А.2.1 Общие положения

А.2.1.1 Элементы структуры

Для выражения своей политики поставщик облачной службы использует все дерево категорий данных, описанное в 6.2.2, но только часть комбинаций действий и областей.

Таблица А.2 — Комбинации действий и областей

Действие	Область
Предоставлять	Приложение/услуга (неявно)
Улучшать	Приложение/услуга Продукты и услуги CSP
Персонализировать	Приложение/услуга Продукты и услуги CSP
Предлагать обновление или дополнительные возможности	Приложение/услуга Продукты и услуги CSP
Продавать, рекламировать, продвигать	Продукты и услуги CSP Сторонние продукты и услуги
Делиться	Сторонние партнеры/обработчики Сторонние продукты и услуги

А.2.1.2 Упрощения структуры спецификации использования данных

Поставщик облачной службы использует определенные упрощения структуры спецификации использования данных:

- несколько элементов структуры одного типа, таких как категории данных, действия или области, могут встречаться последовательно разделенные словом «и» или запятой («,»). Спецификации использования данных, которые содержат такие последовательности, могут быть развернуты в несколько спецификаций использования данных, по одной для каждого элемента. Например, спецификацию использования данных:

> Данные контента клиента и производные данные передаются сторонним партнерам и обработчикам

можно разбить на две спецификации:

> Данные контента клиента передаются сторонним партнерам и обработчикам.
> Производные данные передаются сторонним партнерам и обработчикам.

Такое синтаксическое упрощение можно использовать как для действий, так и для областей;

- перечисление всех элементов категории данных, с учетом нескольких исключений, приводит к очень длинным спецификациям использования данных или, если использовать описанное выше упрощение, к большому числу спецификаций использования данных. Словосочетание «за исключением» используется для обозначения исключений из категорий данных, т. е. запись:

> Данные контента клиента, за исключением учетных данных, передаются сторонним партнерам и обработчикам

можно развернуть в более длинную спецификацию использования данных:

> Списки контактов клиентов, персональные данные о здоровье и медицинские записи, персональные генетические данные, персональные биометрические данные, персональные данные детей, политические взгляды и финансовые данные передаются сторонним партнерам и обработчикам.

Следует отметить, что указанные упрощения могут быть преобразованы в структуру, описанную в настоящем стандарте, без изменения сути спецификации использования данных. Они используются исключительно как упрощения, чтобы сделать вариант использования более читабельным.

А.2.2 Идентифицируемые данные

Поставщик облачной службы может представить свои политики использования идентифицируемых данных в виде приведенной на рисунке А.1 таблицы.

ИДЕНТИФИЦИРОВАННЫЕ ДАННЫЕ			Действия и области										
			Предоставлять	Улучшить		Персонализировать		Предлагать обновления или дополнительные возможности		Продавать, рекламировать, продвигать		Делиться	
Категории данных				Приложение/услуга	Продукты/услуги CSP	Приложение/услуга	Продукты/услуги CSP	Приложение/услуга	Продукты/услуги CSP	Продукты/услуги CSP	Сторонние продукты/услуги	Сторонние продукты/обработчики	Сторонние продукты/услуги
Данные контента клиента	Учетные данные		D-N-A	X	X	X	X	X	X	X	X	D-N-A	P-O-B
	Списки контактов клиентов		D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	X	X	D-N-A	P-O-B
	Персональные медицинские данные и медицинские записи		P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
	Персональные генетические данные		P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
	Персональные биометрические данные		P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
	Персональные данные детей		P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
	Политические взгляды		P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
	Финансовые детали		P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
Производные данные	EUII	Данные телеметрии	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Данные о подключении	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Использование возможностей обслуживания	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Демографическая информация	P-N-A	P-N-A	P-N-A	P-N-A	P-O-B	P-N-A	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B

Рисунок А.1 — Пример политик использования идентифицируемых данных

ИДЕНТИФИЦИРОВАННЫЕ ДАННЫЕ			Действия и области											
			Предоставлять	Улучшить		Персонализировать		Предлагать обновления или дополнительные возможности		Продавать, рекламировать, продвигать		Делиться	
Категории данных				Приложение/услуга	Продукты/услуги CSP	Приложение/услуга	Продукты/услуги CSP	Приложение/услуга	Продукты/услуги CSP	Продукты/услуги CSP	Сторонние продукты/услуги	Сторонние продукты/обработчики	Сторонние продукты/услуги
Производные данные	EUII	Данные профилирования	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Данные о потреблении контента	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		История просмотров на стороне клиента	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
		Поисковые команды и запросы	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
		Местоположение пользователя	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
		Социальные дан ные	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Биометрические и медицинские данные	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Контактные данные конечного пользователя	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Данные о среде пользователя	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
	Операционные данные		D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-A	P-O-B

Рисунок А.1, лист 2

ИДЕНТИФИЦИРОВАННЫЕ ДАННЫЕ		Действия и области										
			Улучшить		Персонализировать		Предлагать обновления или дополнительные возможности		Продавать, рекламировать, продвигать		Делиться	
Категории данных		Предоставлять	Приложение/ услуга	Продукты/ услуги CSP	Приложение/ услуга	Продукты/ услуги CSP	Приложение/ услуга	Продукты/ услуги CSP	Продукты/ услуги CSP	Сторонние продукты/ услуги	Сторонние продукты/обработчики	Сторонние продукты/ услуги
Учетные данные	Контактная информация потребителя	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	X	X	X	X	D-N-A	P-O-B
	Данные платежного инструмента	D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-A	P-O-B

Рисунок А.1, лист 3

Из таблицы на рисунке А.1 можно получить следующие спецификации использования данных:

D-N-A: Использование данных не требует согласия, требуется только информативное уведомление, контроля потребителя не требуется:

- для предоставления этого приложения или услуги используются учетные данные;
- для предоставления и персонализации этого приложения или услуги используются списки контактов клиентов;
- для предоставления, улучшения и персонализации приложения или услуги, а также для предложения обновлений и дополнительных возможностей этого приложения или услуги используется идентифицируемая информация конечного пользователя, за исключением демографической информации, истории просмотров на стороне клиента, поисковых команд и запросов, а также местоположения пользователя;
- для предоставления и улучшения приложения или услуги используются операционные данные;
- для предоставления и улучшения приложения или услуги используются данные учетной записи;
- для персонализации приложения или услуги используется контактная информация учетной записи или администрации;
- доступ к данным контента клиента, производным данным и данным учетной записи разделяется со сторонними партнерами и процессами.

D-N-B: Использование данных не требует согласия, требуется только информативное уведомление, требуется контроль потребителя:

- для улучшения и персонализации продуктов и услуг поставщика облачной службы, а также для предложения обновлений, дополнительных продуктов и услуг поставщика облачной службы используются списки контактов клиентов;
- для улучшения продуктов и услуг поставщика облачной службы используется идентифицируемая информация конечного пользователя, за исключением демографической информации, истории просмотров на стороне клиента, поисковых команд и запросов, а также местоположения пользователя;
- для предложения обновлений, дополнительных продуктов и услуг поставщика облачной службы, а также для маркетинга, рекламы и продвижения продуктов и услуг поставщика облачной службы используется идентифицируемая информация конечного пользователя, за исключением демографической информации, истории просмотров на стороне клиента, поисковых команд и запросов, а также местоположения пользователя;
- для маркетинга, рекламы и продвижения сторонних продуктов и услуг используется идентифицируемая информация конечного пользователя, за исключением демографической информации, истории просмотров на стороне клиента, поисковых команд и запросов, а также местоположения пользователя;
- для улучшения продуктов и услуг поставщика облачной службы используются операционные данные;
- для улучшения продуктов и услуг поставщика облачной службы используются данные учетной записи;
- для персонализации продуктов и услуг поставщика облачной службы используется контактная информация учетной записи или администрации.

P-N-A: Для использования данных не требуется согласие, требуется ярко выраженное уведомление, контроль потребителей не требуется:

- для предоставления приложения или услуги используется демографическая информация;

- демографическая информация используется для улучшения и персонализации продуктов и услуг поставщика облачной службы, а также для предложения обновлений, дополнительных возможностей и услуг поставщика облачной службы.

P-O-B: Для использования данных требуется согласие, требуется ярко выраженное уведомление, требуется контроль потребителей:

- для предоставления этого приложения или услуги используются данные контента клиента, за исключением учетных данных и списков контактов клиентов;
- для улучшения, персонализации, продвижения, рекламы и продвижения продуктов и услуг поставщика облачной службы, а также для предложения обновлений, дополнительных возможностей и услуг поставщика облачной службы используются данные о контенте клиентов, за исключением учетных данных и списков контактов клиентов;
- для маркетинга, рекламы или продвижения сторонних продуктов и услуг используются данные контента клиента, за исключением учетных данных и списков контактов клиентов;
- для персонализации и маркетинга, рекламы и продвижения продуктов и услуг поставщика облачной службы, а также для предложения обновлений и продаж продуктов и услуг поставщика облачной службы используется демографическая информация;
- демографическая информация используется для маркетинга, рекламы и продвижения сторонних продуктов и услуг;
- для предоставления приложения или услуги используются история просмотров на стороне клиента, поисковые команды и запросы, а также местоположение пользователя;
- для улучшения, персонализации и маркетинга, рекламы и продвижения продуктов и услуг поставщика облачной службы, а также для предложения обновлений, дополнительных возможностей и услуг поставщика облачной службы используются история просмотров на стороне клиента, поисковые команды и запросы, а также местоположение пользователя;
- для маркетинга, рекламы и продвижения сторонних продуктов и услуг используются история просмотров на стороне клиента, поисковые команды и запросы, а также местоположение пользователя;
- данные контента клиента, производные данные и данные учетной записи передаются сторонним продуктам и услугам.

А.2.3 Псевдонимизированные данные

Поставщик облачной службы может представить свои политики использования псевдонимизированных данных в виде приведенной на рисунке А.2 таблицы.

Из таблицы на рисунке А.2 можно получить следующие спецификации использования данных:

D-N-A: Использование данных не требует согласия, требуется только информативное уведомление, контроля потребителя не требуется:

- псевдонимизированные учетные данные используются для улучшения приложения или сервиса;
- псевдонимизированные списки контактов клиентов используются для персонализации продуктов и услуг поставщика облачной службы, а также для предложения обновлений, дополнительных возможностей и услуг поставщика облачной службы;
- псевдонимизированная идентифицируемая информация конечного пользователя, за исключением истории просмотров на стороне клиента и местоположения пользователя, используется для предоставления и улучшения этого приложения или услуги, а также для предложения обновлений или дополнительных возможностей услуги;
- псевдонимизированные данные контента клиентов, за исключением учетных данных и списков контактов клиентов, а также производные данных и данных об учетных записях, передаются сторонним партнерам и обработчикам.

D-N-B: Использование данных не требует согласия, требуется только информативное уведомление, требуется контроль потребителя:

- псевдонимизированные учетные данные используются для улучшения продуктов и услуг поставщика облачной службы;
- псевдонимизированные списки контактов клиентов используются для персонализации продуктов и услуг поставщика облачной службы, а также для предложения обновлений, дополнительных возможностей и услуг поставщика облачной службы;
- псевдонимизированная идентифицируемая информация конечного пользователя, за исключением истории просмотров на стороне клиента и местоположения пользователя, используется для персонализации и улучшения, а также для продвижения, рекламы или продвижения продуктов и услуг поставщика облачной службы, а также для предложения обновлений, дополнительных возможностей и услуг поставщика облачной службы;
- псевдонимизированные операционные данные используются для улучшения продуктов и услуг поставщика облачной службы;
- псевдонимизированные данные учетной записи используются для улучшения продуктов и услуг поставщика облачной службы;
- псевдонимизированная идентифицирующая информация конечного пользователя, за исключением истории просмотров на стороне клиента и местоположения пользователя, используется для маркетинга, рекламы или продвижения сторонних продуктов и услуг.

ПСЕВДОНИМИЗИРОВАННЫЕ ДАННЫЕ			Действия и области										
			Предоставлять	Улучшить		Персонализировать		Предлагать обновления или дополнительные возможности		Продавать, рекламировать, продвигать		Делиться	
Категории данных				Приложение/услуга	Продукты/услуги CSP	Приложение/услуга	Продукты/услуги CSP	Приложение/услуга	Продукты/услуги CSP	Продукты/услуги CSP	Сторонние продукты/услуги	Сторонние продукты/обработчики	Сторонние продукты/услуги
Данные контента клиента	Учетные данные		X	D-N-A	D-N-B	X	X	X	X	X	X	X	X
	Списки контактов клиентов		X	X	X	D-N-A	D-N-B	D-N-A	D-N-B	X	X	X	X
	Персональные медицинские данные и записи		P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
	Персональные генетические данные		P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
	Персональные биометрические данные		P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
	Персональные данные детей		P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
	Политические взгляды		P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
	Финансовые детали		P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
Производные данные	EUII	Данные телеметрии	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Данные о подключении	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Использование возможностей обслуживания	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Демографическая информация	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B

Рисунок А.2 — Пример политик использования идентифицируемых данных

ПСЕВДОНИМИЗИРОВАННЫЕ ДАННЫЕ			Действия и области										
			Предоставлять	Улучшить		Персонализировать		Предлагать обновления или дополнительные возможности		Продавать, рекламировать, продвигать		Делиться	
Категории данных				Приложение/услуга	Продукты/услуги CSP	Приложение/услуга	Продукты/услуги CSP	Приложение/услуга	Продукты/услуги CSP	Продукты/услуги CSP	Сторонние продукты/услуги	Сторонние продукты/обработчики	Сторонние продукты/услуги
Производные данные	EUII	Данные профилирования	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Данные о потреблении контента	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		История просмотров на стороне клиента	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
		Поисковые команды и запросы	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Местоположение пользователя	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	P-O-B	D-N-A	P-O-B
		Социальные данные	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Биометрические и медицинские данные	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Контактные данные конечного пользователя	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
		Данные о среде пользователя	D-N-A	D-N-A	D-N-B	D-N-A	D-N-B	D-N-A	D-N-B	D-N-B	D-N-B	D-N-A	P-O-B
	Операционные данные		D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-A	P-O-B

Рисунок А.2, лист 2

ПСЕВДОНИМИЗИРОВАННЫЕ ДАННЫЕ		Действия и области										
		Предоставлять	Улучшить		Персонализировать		Предлагать обновления или дополнительные возможности		Продавать, рекламировать, продвигать		Делиться	
Категории данных			Приложение/услуга	Продукты/услуги CSP	Приложение/услуга	Продукты/услуги CSP	Приложение/услуга	Продукты/услуги CSP	Продукты/услуги CSP	Сторонние продукты/услуги	Сторонние продукты/обработчики	Сторонние продукты/услуги
Учетные данные	Контактная информация потребителя	D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-A	P-O-B
	Данные платежного инструмента	X	D-N-A	D-N-B	X	X	X	X	X	X	D-N-A	P-O-B

Рисунок А.2, лист 3

P-O-B: Для использования данных требуется согласие, требуется ярко выраженное уведомление, требуется контроль потребителей:

- для предоставления приложения или услуги используются псевдонимизированные данные контента клиентов, за исключением учетных данных и списков контактов клиентов;
- псевдонимизированная история просмотров на стороне клиента и местоположение пользователя используются для предоставления приложения или услуги;
- псевдонимизированные данные контента клиентов, за исключением учетных данных и списков контактов клиентов, используются для улучшения и продвижения, рекламы или продвижения продуктов и услуг поставщика облачной службы, а также для предложения обновлений и продаж продуктов и услуг поставщика облачной службы;
- псевдонимизированная история просмотров на стороне клиента и местоположение пользователя используются для улучшения и продвижения, рекламы или продвижения продуктов и услуг поставщика облачной службы, а также для предложения обновлений, дополнительных возможностей и услуг поставщика облачной службы;
- псевдонимизированные данные о клиентах, за исключением учетных данных и списков контактов клиентов, используются для продвижения, рекламы или продвижения сторонних продуктов и услуг;
- псевдонимизированная история просмотров на стороне клиента и местоположение пользователя используются для продвижения, рекламы или продвижения сторонних продуктов и услуг;
- псевдонимизированные данные контента клиентов, за исключением учетных данных и списка контактов клиентов, передаются сторонним продуктам и услугам;
- псевдонимизированные производные данные и данные учетной записи передаются сторонним продуктам и услугам.

А.2.4 Несвязанные псевдонимизированные данные

Поставщик облачной службы может представить свои политики использования несвязанных псевдонимизированных данных в виде приведенной на рисунке А.3 таблицы.

НЕСВЯЗАННЫЕ ПСЕВДОНИМИЗИРОВАННЫЕ ДАННЫЕ			Действия и области										
			Предоставлять	Улучшить		Персонализировать		Предлагать обновление или дополнительные возможности		Продавать, рекламировать, продвигать		Делиться	
Категория данных				Приложение/услуга	Продукты/услуги CSP	Приложение/услуга	Продукты/услуги CSP	Приложение/услуга	Продукты/услуги CSP	Продукты/услуги CSP	Сторонние продукты/услуги	Сторонние продукты/обработчики	Сторонние продукты/услуги
Данные контента клиента	Учетные данные		X	D-N-A	D-N-B	X	X	X	X	X	X	X	X
	Списки контактов клиентов		X	X	X	X	X	X	X	X	X	X	X
	Персональные медицинские данные и записи		D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-A	D-N-B
	Персональные генетические данные		D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-A	D-N-B
	Персональные биометрические данные		D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-A	D-N-B
	Персональные данные детей		D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-A	D-N-B
	Политические взгляды		D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-A	D-N-B
	Финансовые детали		D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-A	D-N-B
Производные данные	EUII	Данные телеметрии	D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-B	P-O-B
		Данные о подключении	D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-B	P-O-B
		Использование возможностей обслуживания	D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-B	P-O-B
		Демографическая информация	D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-B	P-O-B
		Данные профилирования	D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-B	P-O-B
		Данные о потреблении контента	D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-B	P-O-B

Рисунок А.3 — Пример политик использования несвязанных псевдонимизированных данных

НЕСВЯЗАННЫЕ ПСЕВДОНИМИЗИРОВАННЫЕ ДАННЫЕ			Действия и области										
			Предоставлять	Улучшить		Персонализировать		Предлагать обновление или дополнительные возможности		Продавать, рекламировать, продвигать		Делиться	
Категория данных				Приложение/услуга	Продукты/услуги CSP	Приложение/услуга	Продукты/услуги CSP	Приложение/услуга	Продукты/услуги CSP	Продукты/услуги CSP	Сторонние продукты/услуги	Сторонние продукты/обработчики	Сторонние продукты/услуги
Производные данные	EUII	История просмотров на стороне клиента	D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-B	P-O-B
		Поисковые команды и запросы	D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-B	P-O-B
		Местоположение пользователя	X	X	X	X	X	X	X	X	X	D-N-B	P-O-B
		Социальные данные	D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-B	P-O-B
		Биометрические и медицинские данные	D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-B	P-O-B
		Контактные данные конечного пользователя	D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-B	P-O-B
		Данные о среде пользователя	D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-B	P-O-B
	Операционные данные		D-N-A	D-N-A	D-N-B	X	X	X	X	X	X	D-N-A	D-N-B
Учетные данные	Контактная информация для потребителя		X	X	X	X	X	X	X	X	X	D-N-A	X
	Данные платежного инструмента		X	X	X	X	X	X	X	X	X	D-N-A	X

Рисунок А.3, лист 2

D-N-A: Использование данных не требует согласия, требуется только информативное уведомление, контроля потребителя не требуется:

- несвязанные псевдонимизированные данные содержимого клиента, за исключением учетных данных и списков контактов клиентов, а также несвязанная псевдонимизированная идентифицирующая информация конечного

пользователя, за исключением местоположения пользователя, используется для предоставления и улучшения приложения или услуги;

- несвязанные псевдонимизированные данные контента клиента, несвязанные псевдонимизированные производные данные и несвязанные псевдонимизированные данные учетной записи передаются сторонним партнерам и обработчикам.

D-N-B: Использование данных не требует согласия, требуется только информативное уведомление, требуется контроль потребителя:

- несвязанные псевдонимизированные данные контента клиентов, за исключением списков контактов клиентов и несвязанные псевдонимизированные идентифицирующие данные конечных пользователей, за исключением местоположения пользователя, используются для улучшения продуктов и услуг поставщика облачной службы;

- несвязанные псевдонимизированные данные контента клиента и несвязанная псевдонимизированная идентифицирующая информация конечного пользователя передаются сторонним продуктам и услугам.

А.2.5 Анонимизированные и агрегированные данные

Поставщик облачной службы может представить свои политики использования анонимизированных и агрегированных данных в виде приведенной на рисунке А.4 таблицы.

D-N-A: Использование данных не требует согласия, требуется только информативное уведомление, контроля потребителя не требуется:

- анонимизированные или агрегированные производные данные используются для предоставления приложения или услуги;

- анонимизированные или агрегированные производные данные используются для улучшения продуктов и услуг поставщика облачной службы;

- анонимизированные или агрегированные производные данные передаются третьим сторонам и обработчикам, а также сторонним продуктам и услугам.

АНОНИМИЗИРОВАННЫЕ/ АГРЕГИРОВАННЫЕ ДАННЫЕ		Действия и области										
		Предоставлять	Улучшить		Персонализировать		Предлагать обновление или дополнительные возможности		Продавать, рекламировать, продвигать		Делиться	
Категория данных			Приложение/ услуга	Продукты/ услуги CSP	Приложение/ услуга	Продукты/ услуги CSP	Приложение/ услуга	Продукты/ услуги CSP	Продукты/ услуги CSP	Сторонние продукты/ услуги	Сторонние продукты/ обработчики	Сторонние продукты/ услуги
Данные контента	Учетные данные	X	X	X	X	X	X	X	X	X	D-N-A	D-N-A
	Списки контактов клиентов	X	X	X	X	X	X	X	X	X	D-N-A	D-N-A
	Персональные медицинские данные и записи	X	X	X	X	X	X	X	X	X	D-N-A	D-N-A
	Персональные генетические данные	X	X	X	X	X	X	X	X	X	D-N-A	D-N-A
	Персональные биометрические данные	X	X	X	X	X	X	X	X	X	D-N-A	D-N-A
	Персональные данные детей	X	X	X	X	X	X	X	X	X	D-N-A	D-N-A
	Политические взгляды	X	X	X	X	X	X	X	X	X	D-N-A	D-N-A
	Финансовые детали	X	X	X	X	X	X	X	X	X	D-N-A	D-N-A

Рисунок А.4 — Пример политик использования анонимизированных и агрегированных данных

АНОНИМИЗИРОВАННЫЕ/ АГРЕГИРОВАННЫЕ ДАННЫЕ			Действия и области											
			Предоставлять	Улучшить		Персонализировать		Предлагать обновление или дополнительные возможности		Продавать, рекламировать, продвигать		Делиться	
Категория данных				Приложение/ услуга	Продукты/ услуги CSP	Приложение/ услуга	Продукты/ услуги CSP	Приложение/ услуга	Продукты/ услуги CSP	Продукты/ услуги CSP	Сторонние продукты/ услуги	Сторонние продукты/ обработчики	Сторонние продукты/ услуги
Производные данные	EUII	Данные телеметрии	D-N-A	D-N-A	D-N-A	X	X	X	X	X	X	D-N-A	D-N-A
		Данные о подключении	D-N-A	D-N-A	D-N-A	X	X	X	X	X	X	D-N-A	D-N-A
		Использование возможностей обслуживания	D-N-A	D-N-A	D-N-A	X	X	X	X	X	X	D-N-A	D-N-A
		Демографическая информация	D-N-A	D-N-A	D-N-A	X	X	X	X	X	X	D-N-A	D-N-A
		Данные профилирования	D-N-A	D-N-A	D-N-A	X	X	X	X	X	X	D-N-A	D-N-A
		Данные о потреблении контента	D-N-A	D-N-A	D-N-A	X	X	X	X	X	X	D-N-A	D-N-A
		История просмотров на стороне клиента	D-N-A	D-N-A	D-N-A	X	X	X	X	X	X	D-N-A	D-N-A
		Поисковые команды и запросы	D-N-A	D-N-A	D-N-A	X	X	X	X	X	X	D-N-A	D-N-A
		Местоположение пользователя	D-N-A	D-N-A	D-N-A	X	X	X	X	X	X	D-N-A	D-N-A
		Социальные данные	D-N-A	D-N-A	D-N-A	X	X	X	X	X	X	D-N-A	D-N-A
		Биометрические и медицинские данные	D-N-A	D-N-A	D-N-A	X	X	X	X	X	X	D-N-A	D-N-A
		Контактные данные конечного пользователя	D-N-A	D-N-A	D-N-A	X	X	X	X	X	X	D-N-A	D-N-A

Рисунок А.4, лист 2

АНОНИМИЗИРОВАННЫЕ/ АГРЕГИРОВАННЫЕ ДАННЫЕ			Действия и области											
			Предоставлять	Улучшить		Персонализировать		Предлагать обновление или дополнительные возможности		Продавать, рекламировать, продвигать		Делиться	
Категория данных				Приложение/ услуга	Продукты/ услуги CSP	Приложение/ услуга	Продукты/ услуги CSP	Приложение/ услуга	Продукты/ услуги CSP	Продукты/ услуги CSP	Сторонние продукты/ услуги	Сторонние продукты/ обработчики	Сторонние продукты/ услуги
Производные данные	EUII	Данные о среде пользователя	D-N-A	D-N-A	D-N-A	X	X	X	X	X	X	D-N-A	D-N-A
	Операционные данные		D-N-A	D-N-A	D-N-A	X	X	X	X	X	X	D-N-A	D-N-A
Учетные данные	Контактная информация потребителя		X	X	X	X	X	X	X	X	X	D-N-A	D-N-A
	Данные платежного инструмента		X	X	X	X	X	X	X	X	X	D-N-A	D-N-A

Рисунок А.4, лист 3

Библиография

[1] ИСО/МЭК 19944:2017 Информационная технология. Облачные вычисления. Облачные службы и устройства, использующие облачные службы. Поток данных, категории данных и их использование (Information technology — Cloud computing — Cloud services and devices: Data flow, data categories and data use)

[2] Федеральный закон от 27 июля 2006 г. № 149-ФЗ Об информации, информационных технологиях и о защите информации (с изменениями на 30 декабря 2021 г.)

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

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

[5] ИСО/МЭК 38505-2:2018 Информационная технология. Стратегическое управление ИТ. Стратегическое управление данными. Часть 2. Последствия применения ISO/IEC 38500 для менеджмента данных (Information technology — Governance of IT — Governance of data — Part 2: Implications of ISO/IEC 38505-1 for data management)

УДК 006.034:004.056.5:006.354 ОКС 35.210

Ключевые слова: персональные данные, политики данных, категории данных, поставщик облачной службы, потребитель облачных служб, таксономия

Редактор *Л.В. Коретникова*
Технический редактор *В.Н. Прусакова*
Корректор *О.В. Лазарева*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 18.08.2022. Подписано в печать 19.09.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 6,05. Уч.-изд. л. 5,45.

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