Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1363

(05/2020)

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

Безопасные приложения и услуги (2) –
Безопасность интернета вещей (IoT)

Техническая структура обработки информации, позволяющей установить личность, в среде интернета вещей

Рекомендация МСЭ-Т X.1363

ITU-T

ITU Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	**X.1360–X.1369**
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1379
Безопасность технологии распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
БЕЗОПАСНОСТЬ СЕТЕЙ 5G	X.1800–X.1819

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

Рекомендация МСЭ-Т X.1363

Техническая структура обработки информации, позволяющей установить личность, в среде интернета вещей

Резюме

Устройства интернета вещей (IoT) могут собирать данные многих видов, в том числе информацию, позволяющую установить личность (PII). Данные PII требуются в услугах различных типов, поэтому они могут использоваться несколькими поставщиками услуг.

Пользователям в среде IoT целесообразно управлять своими собственными данными, в том числе PII, исходя из своих намерений. Использование данных в среде IoT, где действует большое число поставщиков услуг, сопряжено с трудностями, поэтому следует обеспечить гибкое соответствие намерениям пользователей в отношении использования данных. Например, если поставщик услуг IoT обеспечивает перечисленные ниже функции, пользователь может признать, что поставщик услуг собирает данные и управляет ими (в том числе PII) надлежащим образом.

– Пользователи могут настраивать собственные предпочтения в отношении своей PII. Такие настройки включают перечень данных, которые разрешено использовать совместно с другими поставщиками услуг.
– Сбор и совместное использование данных осуществляются при условии контролируемого доступа на основе настроек PII. Данные, на которые не дано разрешение, не могут помещаться в хранилище данных и не могут использоваться совместно с другими поставщиками услуг.
– Пользователи могут проверять хронологический журнал регистрации совместного использования данных несколькими поставщиками услуг. Пользователи могут также проверять, в какое время осуществлялось совместное использование данных.

В Рекомендации МСЭ-Т X.1363 определена техническая структура обработки PII в среде IoT с одним или несколькими поставщиками услуг.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1363	29.05.2020 года	17-я	11.1002/1000/14087

Ключевые слова

Интернет вещей (IoT); информация, позволяющая установить личность (PII).

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

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

© ITU 2020

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1363

Техническая структура обработки информации, позволяющей установить личность, в среде интернета вещей

1 Сфера применения

В настоящей Рекомендации определена техническая структура обработки информации, позволяющей установить личность (PII), в среде интернета вещей (IoT).

В среде IoT некоторые устройства IoT имеют возможность собирать данные PII. Данные PII требуются в услугах различных типов, поэтому они могут использоваться несколькими поставщиками услуг. Описанная в настоящей Рекомендации техническая структура обеспечивает механизм защиты данных PII пользователей IoT, когда один или несколько поставщиков услуг IoT собирают и используют эти данные или обмениваются ими.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.1058] Рекомендация МСЭ-Т X.1058 (2017 г.) | ИСО/МЭК 29151:2017, *Информационные технологии – Методы обеспечения безопасности – Свод правил и норм для защиты информации, позволяющей установить личность*.

[ISO/IEC 29100] ИСО/МЭК 29100:2011, *Информационная технология. Методы и средства обеспечения безопасности. Концепция защиты персональных данных*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 аутентификация (authentication) [b-ISO/IEC 27000] – обеспечение гарантии правильности заявленной характеристики объекта.

3.1.2 управление доступом (access control) [b-ISO/IEC 10027] – возможность ограничить использование услуг, имеющих доступ к данным, только теми пользователями, которые предварительно были авторизованы.

3.1.3 управление (control) [b-ISO/IEC 27000] – мера, которая изменяет **риск** (3.1.16).

ПРИМЕЧАНИЕ 1. − Средства управления включают любой **процесс** (3.1.15), **политику** (3.1.14), устройство, практику или иные действия, изменяющий **риск** (3.1.16).

ПРИМЕЧАНИЕ 2. − Возможно, что средства управления не всегда оказывают желаемое или предполагаемое воздействие.

3.1.4 устройство (device) [b-ITU-T Y.4000] – применительно к интернету вещей это элемент оборудования, обладающий обязательными возможностями связи и дополнительными возможностями измерения, срабатывания, а также ввода, хранения и обработки данных.

3.1.5 интернет вещей (Internet of things, IoT) [b-ITU-T Y.4000] – глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий.

ПРИМЕЧАНИЕ 1. – Благодаря задействованию возможностей идентификации, сбора, обработки и передачи данных в IoT обеспечивается наиболее эффективное использование вещей для предоставления услуг для всех типов приложений при одновременном выполнении требований безопасности и неприкосновенности частной жизни.

ПРИМЕЧАНИЕ 2. – В широком смысле IoT можно воспринимать как концепцию, имеющую технологические и социальные последствия.

3.1.6 система управления (management system) [b-ISO/IEC 27000] – совокупность взаимосвязанных и взаимодействующих элементов **организации** (3.1.10) для установления **политики** (3.1.14), **целей** (3.1.7) и **процессов** (3.1.15), необходимых для достижения этих целей.

ПРИМЕЧАНИЕ 1. − Система управления может охватывать одну или несколько областей.

ПРИМЕЧАНИЕ 2. − К элементам системы относятся структура, функции и обязанности, планирование и функционирование организации.

ПРИМЕЧАНИЕ 3. − Сфера действия системы управления может включать всю организацию, конкретные и установленные функции организации, конкретные и установленные подразделения организации либо одну или несколько функций группы организаций.

3.1.7 цель (objective) [b-ISO/IEC 27000] – результат, который должен быть достигнут.

ПРИМЕЧАНИЕ 1. − Цель может быть стратегической, тактической или оперативной.

ПРИМЕЧАНИЕ 2. − Цели могут относиться к разным областям (например, цели в области финансов, здравоохранения и безопасности, экологические цели) и применяться на разных уровнях [стратегический уровень, уровень организации, проекта, продукта и **процесса** (3.1.15)].

ПРИМЕЧАНИЕ 3. − Цель может быть выражена другими способами, например в качестве желательного результата, назначения, операционного критерия, цели информационной безопасности или путем использования иных слов аналогичного значения (например, замысел, задача или задание).

ПРИМЕЧАНИЕ 4. − В контексте систем управления информационной безопасностью цели информационной безопасности устанавливает организация в соответствии с политикой информационной безопасности для достижения конкретных результатов.

3.1.8 согласие (opt-in) [b-ISO/TS 17975] – процесс или тип политики, в соответствии с которыми субъект данных должен предпринять отдельное действие, для того чтобы выразить конкретное, явное или предварительное согласие с определенным типом обработки.

3.1.9 отказ (opt-out) [b-ISO/TS 17975] – процесс или тип политики, в соответствии с которыми субъект данных должен предпринять отдельное действие, для того чтобы отозвать или аннулировать согласие на определенный тип обработки.

ПРИМЕЧАНИЕ. − В случае отказа существует подразумеваемое согласие на обработку личной информации организацией, выполняющей сбор, если только лицо явно не выразило отказ или не аннулировало разрешение. Отказ также является процессом, который обеспечивает выполняющая сбор организация, для того чтобы субъект данных мог выразить отказ от определенного типа обработки или аннулировать разрешение на определенный тип обработки.

3.1.10 организация (organization) [b-ISO/IEC 27000] – отдельное лицо или группа лиц, которые имеют собственные функции, а также обязанности, полномочия и взаимоотношения для достижения своих **целей** (3.1.7).

ПРИМЕЧАНИЕ. − Понятие организации включает, в том числе, индивидуального предпринимателя, компанию, корпорацию, фирму, предприятие, орган, партнерство, благотворительное общество, учреждение либо их части или сочетание, независимо от того, являются или не являются они юридическим лицом, государственной или частной структурой.

3.1.11 информация, позволяющая установить личность (personally identifiable information, PII) [ISO/IEC 29100] – любая информация, которая а) может быть использована для идентификации

субъекта PII, к которому такая информация относится, или b) прямо или косвенно связана либо может быть связана с субъектом PII.

ПРИМЕЧАНИЕ. – Для определения возможности идентификации субъекта PII следует учесть все способы идентификации этого физического лица, которые, исходя из разумных предположений, может использовать заинтересованное лицо, хранящее данные, или любая другая сторона.

3.1.12 настройки, относящиеся к информации, позволяющей установить личность (personally identifiable information preferences) [ISO/IEC 29100] – конкретные настройки, которые определил субъект информации, позволяющей установить личность (PII), в отношении порядка обработки своей PII для конкретного назначения.

3.1.13 субъект информации, позволяющей установить личность (personally identifiable information principal) [ISO/IEC 29100] – физическое лицо, к которому относится информация, позволяющая установить личность (PII).

ПРИМЕЧАНИЕ. – В зависимости от юрисдикции и конкретного закона о защите данных и конфиденциальности, вместо термина "субъект PII" может использоваться также его синоним "субъект данных".

3.1.14 политика (policy) [b-ISO/IEC 27000] – намерения и направление деятельности **организации** (3.1.10), официально определенные ее **руководством высшего звена** (3.1.18).

3.1.15 процесс (process) [b-ISO/IEC 27000] – совокупность взаимосвязанных и взаимовлияющих действий, которая обеспечивает преобразование исходных компонентов в результаты.

3.1.16 риск (risk) [b-ISO/IEC 27000] – влияние неопределенности на **цели** (3.1.7).

3.1.17 вещь (thing) [b-ITU-T Y.4000] – применительно к интернету вещей означает предмет физического мира (физические вещи) или информационного мира (виртуальные вещи), который может быть идентифицирован и интегрирован в сети связи.

3.1.18 руководство высшего звена (top management) [b-ISO/IEC 27000] – лицо или группа лиц, которые осуществляют руководящие и контролирующие функции в отношении **организации** (3.1.10) на высшем уровне.

ПРИМЕЧАНИЕ 1. − Руководство высшего звена имеет право делегировать полномочия и предоставлять ресурсы в рамках организации.

ПРИМЕЧАНИЕ 2. − Если сфера действия **системы управления** (3.1.6) охватывает только часть организации, руководство высшего звена означает тех лиц, которые осуществляют руководящие и контролирующие функции в отношении этой части организации.

ПРИМЕЧАНИЕ 3. − Руководство высшего звена иногда называют исполнительным руководством, и оно может включать главных исполнительных директоров, финансовых директоров, директоров по информационным технологиям и аналогичные должности.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

ACT	Access Control Table	Таблица управления доступом
IoT	Internet of Things	Интернет вещей
PII	Personally Identifiable Information	Информация, позволяющая установить личность
T&C	Terms and Conditions	Положения и условия

5 Соглашения

Отсутствуют.

6 Обзор

Существует большое число различных типов устройств IoT, и некоторые из них имеют возможность собирать данные PII. Данные PII требуются в разнообразных услугах, поэтому поставщики услуг стремятся собирать различные данные PII пользователей. Кроме того, поставщик услуг может использовать эти собранные данные PII вместе с другими поставщиками услуг в целях совместного предоставления услуг, которые в большей степени подходят пользователям. В этом случае существует два типа поставщиков услуг: поставщики, собирающие данные (PII) пользователей, и поставщики, предоставляющие разнообразные услуги, используя данные, которые были собраны другими поставщиками услуг.

С точки зрения пользователей, эти поставщики услуг должны обрабатывать их данные PII надлежащим образом. Пользователям в среде IoT рекомендуется определять свои предпочтения в отношении порядка обработки их данных, в том числе PII. Использование данных в среде IoT, где действует большое число поставщиков услуг, сопряжено с трудностями, поэтому следует обеспечить гибкое соответствие намерениям пользователей в отношении использования данных. Например, если поставщик услуг IoT обеспечивает перечисленные ниже функции, пользователь может признать, что поставщик услуг собирает данные и управляет ими (в том числе PII) надлежащим образом.

– Пользователи могут настраивать собственные предпочтения в отношение своей PII. Такие настройки включают перечень данных, которые разрешено использовать совместно с другими поставщиками услуг.
– Сбор и совместное использование данных осуществляются при условии контролируемого доступа на основе настроек PII. Данные, на которые не дано разрешение, не могут помещаться в хранилище данных и не могут использоваться совместно с другими поставщиками услуг.
– Пользователи могут проверять хронологический журнал регистрации совместного использования данных несколькими поставщиками услуг. Пользователи могут также проверять, в какое время осуществлялось совместное использование данных.

7 Модель услуг IoT с одним или несколькими поставщиками услуг

На рисунке 1 представлена модель услуг IoT, в которой услугу предоставляет один поставщик услуг. В этом случае поставщик услуг собирает данные нескольких типов (включая PII) и сохраняет информацию в хранилище данных, управляемом этим поставщиком услуг. Поставщик услуг предоставляет различные приложения пользователям, которые предоставляют свои данные (включая PII) этому поставщику услуг.

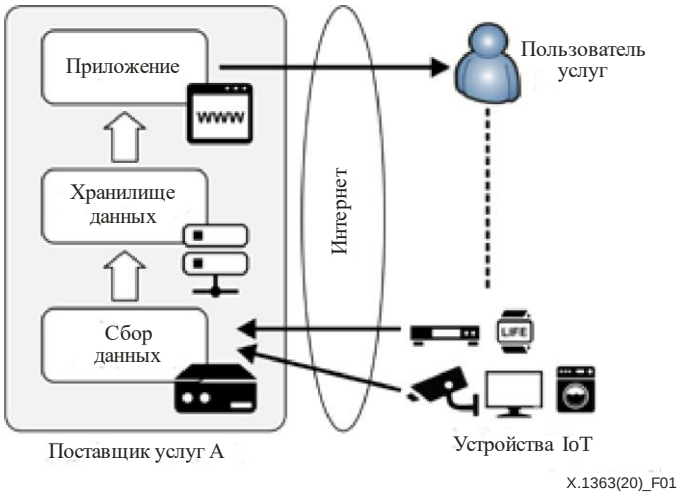

Рисунок 1 – Модель с одним поставщиком услуг

В этой модели услуг IoT собранные данные обрабатывает единственный поставщик услуг, а пользователи используют приложение(я) в соответствии с согласованными положениями и условиями (T&C).

На рисунке 2 представлена модель с несколькими поставщиками услуг, которые совместно используют данные, собранные с устройств IoT. В этом случае существует два вида поставщиков услуг: "поставщик услуг – поставщик данных" и "поставщик услуг – поставщик приложений". На рисунке 2 поставщик услуг A собирает данные (включая PII) с устройств IoT и передает их другим поставщикам услуг (поставщику услуг B и поставщику услуг C). Поставщик услуг A определяется как "поставщик услуг – поставщик данных", а поставщики услуг B и C – как "поставщики услуг – поставщики приложений". Поставщик услуг может быть как "поставщиком услуг – поставщиком данных", так и "поставщиком услуг – поставщиком приложений".

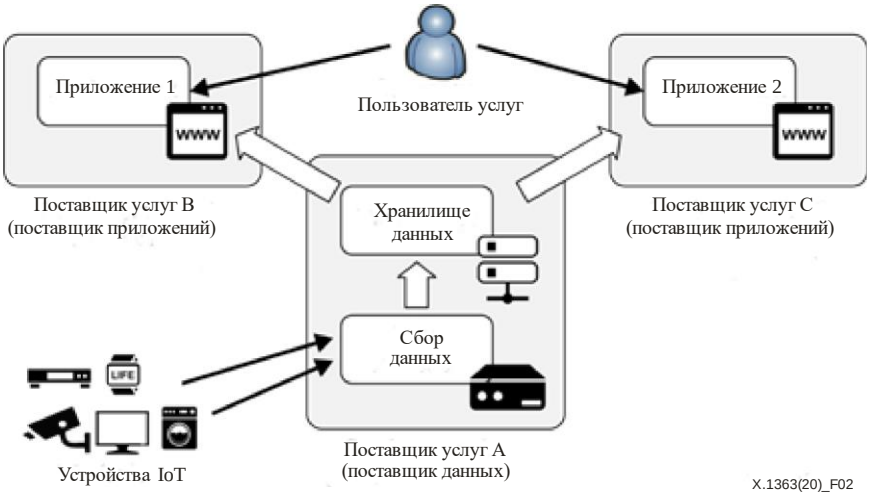

Рисунок 2 – Модель с несколькими поставщиками услуг

Как правило, перечень данных, которые используются совместно с другими поставщиками услуг, включается в T&C поставщика услуг – поставщика данных, и пользователи, прежде чем они смогут использовать услугу (услуги) этого поставщика услуг, должны согласиться с этим перечнем данных.

Основное различие между моделью с одним поставщиком услуг и моделью с несколькими поставщиками услуг заключается в том, используются ли собранные устройствами IoT данные совместно с другими поставщиками услуг – поставщиками приложений. В случае модели с несколькими поставщиками услуг собранные устройствами IoT данные передаются другим поставщикам услуг – поставщикам приложений.

8 Аспекты обработки данных PII услугами IoT

При обработке данных PII поставщики услуг IoT должны учитывать следующие аспекты.

– Назначение сбора данных PII

Во избежание сбора излишних с точки зрения пользователя данных, пользователю необходимо знать назначение сбора данных и характер данных, собираемых для услуги IoT.

– Обязательное согласие на сбор данных PII

При оформлении пользователями подписки на услугу IoT поставщику услуг – поставщику данных необходимо получить согласие пользователей на сбор данных PII нескольких видов. Как правило, эта информация отражается в T&C поставщика услуг – поставщика данных, и пользователи обязаны согласиться с ней до подписки на услугу.

– Передача данных PII третьим сторонам

Данные, собранные с устройств IoT, могут передаваться третьим сторонам, то есть другим поставщикам услуг. В этом случае поставщику услуг – поставщику данных, прежде чем он сможет отправить данные PII другим поставщикам услуг, необходимо получить явно выраженное согласие пользователей на передачу их данных PII третьим сторонам. В большинстве случаев пользователи не имеют возможности управлять передачей данных PII. Например, пользователи не могут ни выбирать третьи стороны, которым они разрешают отправлять свои данные PII, ни определять с помощью настроек, данные какого типа PII могут использоваться совместно. Кроме того, пользователи не имеют возможности узнать, какие данные PII отправляются третьим сторонам.

– Согласие и отказ от согласия на сбор/передачу данных PII

В случае если услуга использует данные PII пользователя, поставщику услуг – поставщику данных необходимо получить согласие пользователя и на сбор данных PII от пользователя, и на передачу этих данных третьей стороне. Важно не только время получения согласия, но и способ его получения (согласие или отказ).

9 Принципы обработки данных PII услугами IoT

Принципы защиты и средства защиты PII определены в [ISO/IEC 29100] и [ITU-T X.1058]; они разработаны на основе различных принципов защиты PII, существующих в ряде стран, регионов и международных организаций, таких как Организация экономического сотрудничества и развития (ОЭСР) и Азиатско-Тихоокеанское экономическое сотрудничество (АТЭС).

В пунктах 9.1 и 9.2 перечислены принципы обработки данных PII услугами IoT, соответствующие принципам, изложенным в [ISO/IEC 29100] и [ITU-T X.1058].

9.1 Общие принципы обработки данных PII услугами IoT

PII может использоваться для идентификации отдельного лица, обращения к нему или определения его местоположения. Раскрытие такой информации может привести к хищению идентификационных данных или иным мошенническим действиям с ними, в результате чего частным лицам будет нанесен значительный вред, созданы препятствия или причинены неудобства [b-GAO-08-343]. В силу этого обработка данных PII услугами IoT должна отвечать следующим общим принципам.

1) Шифрование данных PII

Все данные PII, хранящиеся на устройствах IoT или в базах данных услуг, подлежат шифрованию. Кроме того, все данные PII должны быть зашифрованы во время передачи по всем компонентам услуги IoT и между ними (то есть устройство IoT, хранилище данных и приложение).

2) Управление доступом/аутентификация

В случае если PII хранится на устройствах IoT или в базах данных услуг (хранилище данных), должны применяться надлежащие средства управления доступом. Авторизация для доступа к PII должна быть ограничена исключительно реализацией назначения использования этих данных, согласие на которое запросил поставщик услуг. Это назначение использования должно быть включено в T&C, на которые поставщик услуг получил согласие пользователя. Доступ должен быть ограничен также, если существует вероятность возникновения связи между хранимыми наборами данных, которая приведет к неразрешенному обнаружению или выводу дополнительной PII.

3) Ведение журналов регистрации

Создание машиночитаемых выборок данных, содержащих данные PII, должно отражаться в официальном журнале регистрации, где указывается создатель выборки, дата, тип информации, назначение выборки и пользователь. Любая PII, включенная в такие журналы (например, имя пользователя), должна быть зашифрована, а доступ к ней должен быть управляемым.

4) Шифрование при осуществлении связи

Данные PII, если они совместно используются несколькими поставщиками услуг, должны быть зашифрованы или замаскированы.

5) Уведомление о нарушении конфиденциальности данных

В случае если произошло нарушение конфиденциальности данных PII вследствие уязвимости данных, утечки данных, их злонамеренного использования или неправильной обработки в любой точке услуги IoT, поставщик услуги должен сразу же после обнаружения нарушения конфиденциальности уведомить затронутых пользователей и соответствующих поставщиков услуг.

6) Процедуры минимизации данных для хранения

Любое хранение данных PII, собранных или производимых в качестве результата обработки данных, которую выполняет поставщик услуг, должно быть ограничено исключительно конкретным назначением, в отношении которого поставщик услуг получил явное согласие пользователя. Поставщик услуг должен установить максимальный период хранения данных PII, ограниченный с учетом конкретного назначения использования, вероятностью возникновения любой связи между хранимыми наборами данных, которая приведет к обнаружению или выводу дополнительной PII, а также всех применимых национальных законов и нормативных актов.

9.2 Принципы обработки данных PII

Поставщики услуг – поставщики данных, которые собирают данные PII с устройств IoT, должны обрабатывать эти данные надлежащим образом. В частности, если данные используются услугами и совместно используются другими поставщиками услуг, их обработка должна соответствовать намерениям пользователя. В силу этого обработка данных PII услугами IoT должна отвечать следующим общим принципам.

1) Разъяснение назначения сбора данных PII

Для того чтобы собирать от пользователей минимальные необходимые данные PII для предоставления услуги IoT, поставщик услуг должен указать в T&C назначение сбора этих данных и период хранения любой собранной PII.

2) Явно выраженное согласие на сбор и совместное использование данных PII от пользователей

В случае если поставщик услуг предоставляет услуги, которые выполняют сбор данных PII от пользователей, этот поставщик услуг должен получить явное согласие пользователя на сбор и совместное использование таких данных. В частности, для получения согласия поставщик услуг должен реализовать, если это возможно, модель явного согласия.

3) Прозрачность использования данных PII

В случае совместного использования с другими поставщиками услуг данных PII, включая данные PII, производимые в качестве результата обработки данных, которую выполняет поставщик услуг, этот поставщик услуг должен обеспечить прозрачность механизма управления PII, для того чтобы пользователи имели возможность проверять использование собственных данных PII. Услуга IoT должна также обеспечивать механизм исправления, который пользователи могут использовать в случае ошибки отнесения данных.

4) Управление собственными настройками

Обработка данных PII должна выполнять на основе предпочтений в отношении PII, определенных в настройках пользователя.

10 Обработка данных PII в среде IoT

10.1 Базовая структура обработки данных PII в среде IoT

На рисунке 3 показана базовая структура обработки данных PII в среде IoT.

Во-первых, пользователи принимают решение о своих предпочтениях в отношении обработки данных PII и отражают их как свои настройки PII в диспетчере настроек PII. Управление предоставляемыми пользователем данными (включая PII) осуществляется на основе настроек PII.

Настройки PII могут включать следующие элементы:

– виды данных, собираемых устройствами IoT: устройства IoT должны собирать только те данные PII, в отношении которых пользователи дали конкретное согласие в своих настройках PII;

– время выполнения сбора данных устройствами IoT (например, в будние дни с 09 час. 00 мин. до 17 час. 30 мин.): пользователи не хотят, чтобы отправка их данных PII происходила в любой момент, поэтому время ее выполнения необходимо установить в настройках PII;

– разрешенные поставщики услуг, с которыми могут совместно использоваться данные PII: пользователи могут выбирать поставщиков услуг – поставщиков приложений, которые могут получить доступ к их данным PII. Пользователи могут также выбирать виды данных PII, к которым поставщики услуг – поставщики приложений могут получить доступ, включая данные, собираемые с устройств IoT или производимые в качестве результата обработки данных, которую выполняет основной поставщик услуг.

Начиная сбор и использование данных, компоненты услуг IoT, такие как устройство IoT, хранилище данных, приложений и т. д., должны проверять настройки PII и выполнять обработку данных соответствующим образом.

Во-вторых, в соответствии с настройками PII генерируется информация управления доступом, и на основе этой информации обновляется таблица управления доступом (ACT).

В-третьих, каждый компонент, если он собирает или передает данные PII, обращается к этой ACT. На основе содержащейся в ACT информации управления доступом определяется, данные PII какого типа могут передаваться между компонентами услуги IoT.

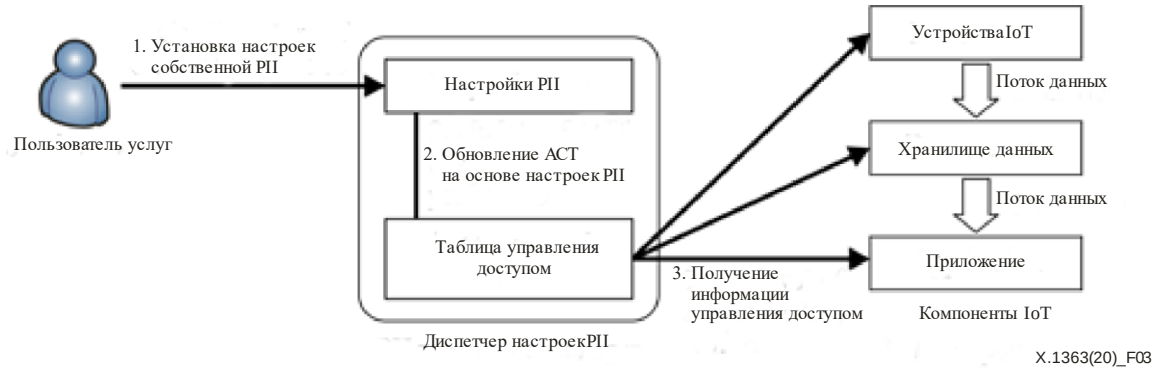

Рисунок 3 – Базовая структура обработки данных PII

10.2 Принципы организации пользовательского интерфейса для установки настроек PII

Для реализации этой базовой структуры поставщики услуг должны обеспечить пользовательский интерфейс, с помощью которого пользователи смогут устанавливать свои настройки PII. Этот пользовательский интерфейс должен отвечать следующим принципам.

1) Простой доступ для всех пользователей

Все пользователи должны иметь возможность простого доступа к пользовательскому интерфейсу. Например, на первом экране предоставляемых услуг должна быть размещена ссылка на этот пользовательский интерфейс.

2) Надлежащее управление доступом к пользовательскому интерфейсу

Все пользователи услуг имеют настройки собственной PII. Следовательно, каждый пользователь должен иметь уникальную учетную запись пользователя и до получения доступа к своей учетной записи пользователя должен проходить аутентификацию защищенным образом, например путем двухфакторной аутентификации.

3) Полнота

Пользовательский интерфейс должен управлять всеми настройками PII, включая сбор и совместное использование PII, одного пользователя в одном месте.

4) Простота использования

Пользовательский интерфейс должен быть простым и очевидным, чтобы дать возможность пользователям установить свои настройки PII.

11 Техническая структура обработки данных PII в среде IoT

В этом разделе показан порядок применения описанной в разделе 10 базовой структуры обработки данных PII в средах с одним поставщиком и с несколькими поставщиками услуг.

11.1 Обработка данных PII услуг IoT одним поставщиком услуг

11.1.1 Эталонная модель предоставления услуг IoT одним поставщиком услуг

На рисунке 4 показана эталонная модель, иллюстрирующая предоставление услуг IoT одним поставщиком услуг. В этом случае один поставщик услуг предоставляет все функции для услуг IoT. Поставщик услуг собирает с устройств IoT данные (включая PII) и сохраняет их в хранилище данных. Используя собранные данные, поставщик услуг может предоставлять пользователям прикладные услуги.

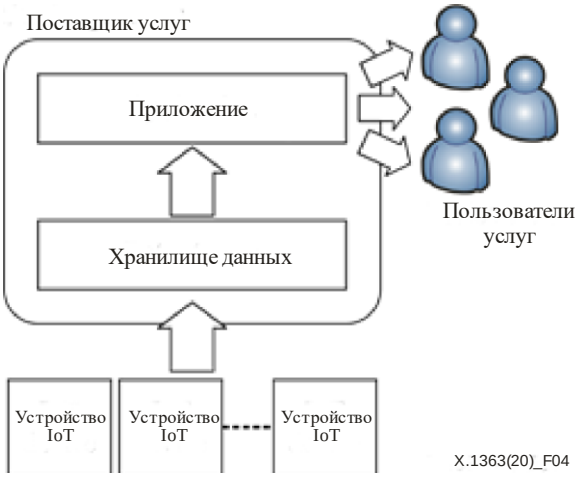

Рисунок 4 – Эталонная модель предоставления услуг IoT одним поставщиком услуг

11.1.2 Техническая структура обработки данных PII одним поставщиком услуг

Техническая структура, приведенная на рисунке 5, представляет поставщика услуг, имеющего диспетчер настроек PII, который управляет настройками PII пользователей. Пользователи

устанавливают настройки своей PII с помощью этого диспетчера настроек PII, и компоненты услуги IoT, такие как устройство IoT, хранилище данных и приложение, обрабатывают данные PII на основе этих настроек. Например, если пользователь желает ввести ограничение на конкретные данные PII, собираемые с устройств IoT, то в результате устройства IoT не должны отправлять такие данные PII в хранилище данных.

Рисунок 5 – Техническая структура обработки данных PII одним поставщиком услуг

11.1.3 Техническая структура обработки данных PII одним поставщиком услуг с порталом управления общими настройками PII

В случае если услуги IoT предоставляет один поставщик, данные, собираемые устройствами IoT, не передаются другим поставщикам услуг, услуги IoT которых этот пользователь не использует. Однако может возникнуть необходимость передать поставщикам услуг некоторые базовые элементы настроек PII, так как установка пользователями своих настроек PII для каждой отдельной услуги IoT может занимать слишком много времени. Если пользователи могут определить общие настройки PII для любого вида услуг IoT, установка настроек PII для каждой отдельной услуги будет проще и эффективнее. Для реализации этого существует два типа диспетчера настроек PII.

На рисунке 6 представлена техническая структура, в которой существует два компонента диспетчера настроек PII; один из них – по-прежнему диспетчер настроек PII, размещенный у поставщика услуг, а второй – портал управления настройками PII, используемый для управления общими настройками для любых услуг IoT и для доступа к этим настройкам других поставщиков услуг.

В этом случае общие настройки пользователя для всех услуг хранятся на портале управления настройками PII, тогда как конкретные настройки пользователя для каждой отдельной услуги хранятся у диспетчера настроек PII, которым управляет поставщик каждой услуги. Когда пользователь начинает подписку на новую услугу, диспетчер локальных настроек PII, находящийся у поставщика услуг – поставщика данных, получает общие настройки этого пользователя из портала управления настройками PII, которым может управлять третья сторона и который пользователь может настроить заранее. Пользователям все еще необходимо установить для данной конкретной услуги свои настройки PII с использованием диспетчера локальных настроек, но они не должны каждый раз устанавливать свои общие настройки, которые хранятся на портале управления настройками PII. Компоненты услуги IoT, такие как устройство IoT, хранилище данных и приложение, управляют данными PII на основе локальных настроек, которые находятся у диспетчера настроек PII.

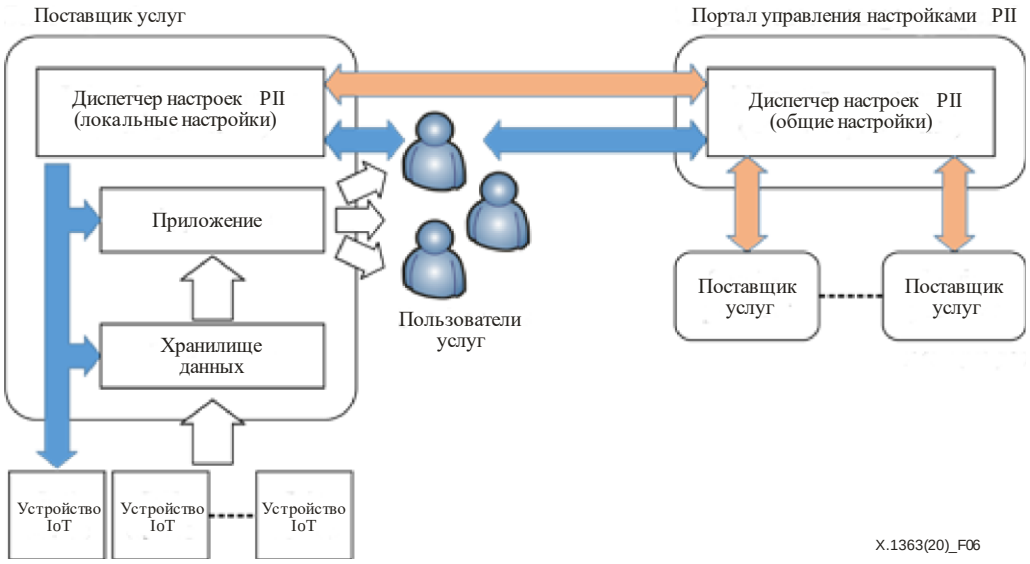

Рисунок 6 – Техническая структура обработки данных PII в услугах IoT одним поставщиком услуг с порталом управления общими настройками PII

11.2 Обработка данных PII услуги IoT несколькими поставщиками услуг

11.2.1 Эталонная модель предоставления услуг IoT несколькими поставщиками услуг

На рисунке 7 представлена эталонная модель, иллюстрирующая предоставление услуг IoT несколькими поставщиками услуг. В этом случае услугу IoT составляют несколько поставщиков услуг (поставщик приложений и поставщик данных), и каждый поставщик услуг – поставщик приложений предоставляет пользователю свою(и) собственную(ые) услугу(и), используя данные, собранные другим поставщиком услуг – поставщиком данных. Следовательно, поставщики услуг, которые собирают данные (включая PII) с устройств IoT (поставщики данных), могут отличаться от поставщиков, которые только предоставляют услуги пользователям (поставщики приложений). На рисунке 7 показаны два типа поставщиков услуг: "поставщик услуг – поставщик данных", который собирает данные (включая PII) с устройств IoT, и "поставщик услуг – поставщик приложений", который предоставляет пользователям прикладные услуги, используя эти собранные данные.

Рисунок 7 – Эталонная модель предоставления услуг IoT несколькими поставщиками услуг

11.2.2 Техническая структура обработки данных PII несколькими поставщиками услуг

На рисунке 8 представлена техническая структура, иллюстрирующая, что у поставщика услуг – поставщика данных имеется диспетчер настроек PII и в этом локальном компоненте управления выполняется управление всеми настройками пользователей, относящимися к обработке данных PII. Компоненты услуг IoT (включая приложения, предоставляемые другими поставщиками услуг – поставщиками приложений) обрабатывают данные PII на основе локальных настроек, которые находятся у диспетчера настроек PII поставщика услуг – поставщика данных.

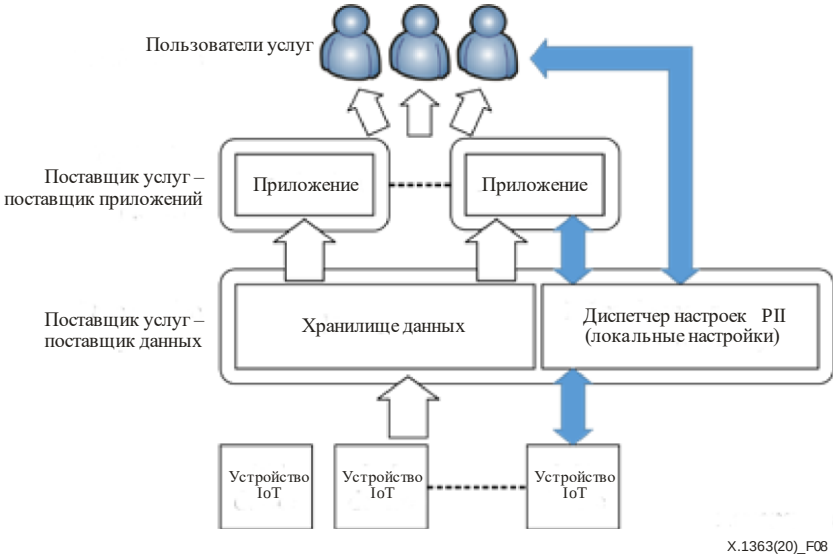

Рисунок 8 – Техническая структура обработки данных PII в услугах IoT несколькими поставщиками услуг

11.2.3 Техническая структура обработки данных PII в услугах IoT несколькими поставщиками услуг с порталом управления общими настройками PII

На рисунке 9 представлена техническая структура, иллюстрирующая, что несколько поставщиков услуг используют настройки PII, которые хранятся как на портале управления общими настройками PII, так и у диспетчеров локальных настроек PII поставщиков услуг – поставщиков данных.

В этом случае общие настройки для любых услуг хранятся на портале управления общими настройками PII, тогда как конкретные настройки для каждой услуги хранятся у диспетчера локальных настроек каждого поставщика услуг – поставщика данных. Когда пользователь начинает подписку на новую услугу, диспетчер локальных настроек PII поставщика услуг получает общие настройки этого пользователя из портала управления настройками PII. Этому пользователю по-прежнему необходимо установить свои настройки PII в диспетчере локальных настроек PII, но он не должен каждый раз настраивать свои общие настройки PII, которые хранятся на портале управления настройками PII. Компоненты услуги IoT управляют данными PII на основе локальных настроек, которые находятся у диспетчера настроек PII.

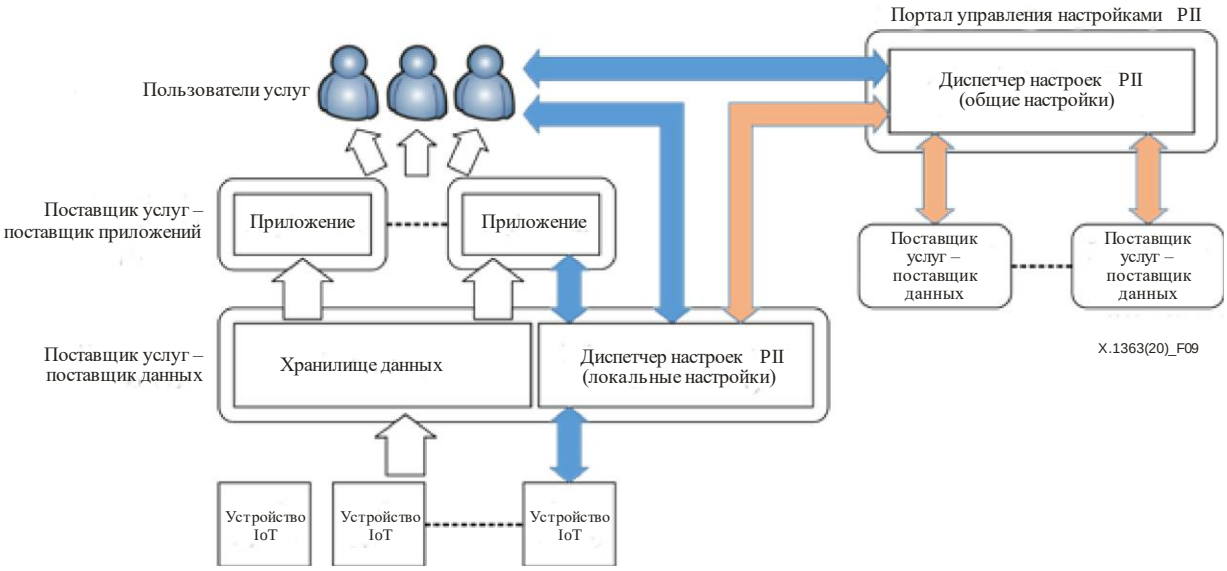

Рисунок 9 – Техническая структура обработки данных PII в услугах IoT несколькими поставщиками услуг с порталом управления общими настройками PII

Библиография

[b-ITU-T Y.4000] Рекомендация МСЭ-Т Y.4000/Y.2060 (2012 г.), *Обзор интернета вещей.*

[b-ISO/IEC 10027] ИСО/МЭК 10027:1990, *Информационная технология. Структура системы словаря информационных ресурсов (IRDS)*.

[b-ISO/IEC 27000] ИСО/МЭК 27000:2018, *Информационная технология – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Общие сведения и словарь*.

[b-ISO/TS 17975] ISO/TS 17975:2015, *Информатика в здравоохранении. Принципы и требования к данным для соглашения о сборе, использовании или разглашении персональной информации о здоровье*.

[b-GAO-08-343] GAO-08-343 (2008). *Information security: Protecting personally identifiable information*. Washington, DC: United States Government Accountability Office. 34 pp.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

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

Отпечатано в Швейцарии
Женева, 2020 год