МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т X.1171

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(02/2009)

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

Безопасные приложения и услуги – Безопасность сетевой идентификации

Угрозы и требования к защите информации, позволяющей установить личность, в приложениях, использующих идентификацию на основе маркеров

Рекомендация МСЭ-Т X.1171

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	
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	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	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339

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

Рекомендация МСЭ-Т X.1171

Угрозы и требования к защите информации, позволяющей установить личность, в приложениях, использующих идентификацию на основе маркеров

Резюме

Широкое применение идентификационных маркеров, в том числе маркеров радиочастотной идентификации (RFID), может вызвать обеспокоенность в отношении нарушения конфиденциальности из-за способности технологии RFID выполнять функции автоматического сбора и обработки данных с возможным раскрытием таких данных неограниченному кругу лиц (преднамеренно или случайно).

Для приложений, использующих идентификацию на базе маркеров и основанных на маркере личной идентификации в персонализированных послепродажных приложениях управления, приложениях, касающихся здравоохранения и т. д., вопрос обеспечения конфиденциальности становится серьезной проблемой. В настоящей Рекомендации описан ряд нарушений информации, позволяющей установить личность (PII), для приложений, в которых используется идентификация на основе маркеров, а также требования по защите PII. Кроме того, в данной Рекомендации приводится базовая структура защиты PII на основе краткого описания правил PII.

Источник

Рекомендация МСЭ-Т X.1171 утверждена 20 февраля 2009 года 17-й Исследовательской комиссией МСЭ-Т (2009–2012 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

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/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1171[1]

Угрозы и требования к защите информации, позволяющей установить личность, в приложениях, использующих идентификацию на основе маркеров

1 Сфера применения

Сфера применения данной Рекомендации охватывает следующие задачи, включающие угрозы и требования к защите информации, позволяющей установить личность (PII), в приложениях, использующих идентификацию на основе маркеров, которые описаны ниже:

– описать угрозы PII в среде, основанной на принципе "бизнес-для-потребителя" (B2C), в приложениях, использующих идентификацию на основе маркеров;

– определить требования к защите PII в среде, основанной на принципе B2C, в приложениях, использующих идентификацию на основе маркеров.

Следующие задачи не входят в сферу применения данной Рекомендации:

– проанализировать общие угрозы безопасности и требования к приложениям, использующим идентификацию на основе маркеров;

– проанализировать угрозы PII и требования между маркером идентификации (ID) и терминалом получения ID;

– проанализировать угрозы PII и требования, обусловленные спецификой маркирования ID и метода считывания, например маркером радиочастотной идентификации и терминала получения ID;

– определить и разработать форматы сообщений и механизмы защиты PII на основе описания политики в приложениях, использующих идентификацию на основе маркеров.

ПРИМЕЧАНИЕ 1. – Потребуется дальнейшая работа, для того чтобы определить такие форматы, которые не будут ограничиваться исключительно защитой PII при использовании идентификации на основе маркеров, но, возможно, с более общим в отношении конфиденциальности подходом.

В данной Рекомендации пользователь маркера ID имеет возможность сам управлять маркером ID, поэтому предполагается, что за работу маркера ID ответственность несет пользователь маркера ID.

ПРИМЕЧАНИЕ 2. – В некоторых случаях пользователь маркер ID не имеет возможности управлять маркером ID. Например, кто-либо покупает маркированную продукцию, и производитель требует сохранять маркер ID действительным на протяжении всего гарантийного срока. В этом случае пользователем маркера ID может быть только лицо, транспортирующее и использующее маркированную продукцию. Таким образом, данная Рекомендация не может быть применена для решения вышеуказанной проблемы для такого случая. Этот случай требует иного законодательства и принципиального подхода (см. [b-OECD]), и этот подход может стать предметом рассмотрения другой Рекомендации.

2 Справочные документы

Нижеследующие Рекомендации МСЭ-Т и другие источники 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 источники являются предметом пересмотра; поэтому всем пользователям данной Рекомендации предлагается рассмотреть возможность применения последнего издания Рекомендаций и других ссылок, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т публикуется регулярно. Ссылка в настоящей Рекомендации на какой-либо документ не придает ему, как отдельному документу, статус рекомендации.

[ITU-T X.1121] Рекомендация МСЭ-Т X.1121 (2004 г.), *Структура технологий безопасности для подвижной связи, обеспечивающей сквозную передачу данных.*

---

[1] Эта Рекомендация не может быть применена в Германии в связи с немецким законодательством.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 управление доступом (access control) [b-ITU-T X.800]: Предотвращение несанкционированного использования какого-либо ресурса, в том числе предотвращение использования ресурса в режиме несанкционированных действий.

3.1.2 сервер приложений (application server) [ITU-T X.1121]: Объект, связывающий отрытую сеть передачи данных с подвижными терминалами.

3.1.3 поставщик прикладных услуг (application service provider (ASP)) [ITU-T X.1121]: Объект (лицо или группа лиц), который предоставляет прикладные услуги подвижным пользователям через сервер приложений.

3.1.4 аутентификация (authentication) [b-ITU-T X.811]: Предоставление гарантий при подтверждении подлинности объекта.

ПРИМЕЧАНИЕ. – Использование слова "идентичность" производится с пониманием того, что в сфере связи это идентификатор или набор идентификаторов, которые подтверждены, что означает, что они были сочтены заслуживающими доверия в результате конкретной работы, произведенной частью сети, терминалом сети или пользователем после завершения процесса одобрения. В том смысле, в котором здесь используется этот термин, нельзя сделать вывод о том, что подтвержденные идентификаторы правильно установят личность.

3.1.5 идентификатор (identifier) [b-ITU-T F.771]: Ряд цифр, знаков и символов или любой другой формы данных, используемых для идентификации физического объекта. Он используется для отображения связи между физическим объектом и информации/признаках о нем в компьютерах. Эта взаимосвязь дает возможность пользователям получать доступ к информации/признакам объекта, содержащейся в компьютерах через терминалы пользователя ID.

3.1.6 маркер ID (ID tag) [b-ITU-T F.771]: Крошечный физический объект, который сохраняет небольшой объем информации, содержащей идентификатор или заключающий в себе опознавательный знак с применением других дополнительных данных, таких как имя, название, цена, и адрес.

3.1.7 терминал получения ID (ID terminal) [b-ITU-T F.771]: Устройство с возможностью ввода данных с маркеров ID и другими возможностями, такими как возможность связи и возможность представления мультимедийной информации. Возможность ввода данных может включать в себя функцию получения идентификатора из маркеров ID, таких как штрих-коды и двумерные (2D) штрих-коды, даже без какой-либо возможности связи. Примеры оборудования, использующего технику для ввода данных: цифровая камера, оптические сканеры, радиопередатчики, IrDA, гальванические проводные линии и т. д.

3.1.8 сеть подвижной связи (mobile network) [ITU-T X.1121]: Сеть, которая предоставляет подвижным терминалам пункты доступа к беспроводной сети.

3.1.9 подвижный терминал (mobile terminal) [ITU-T X.1121]: Объект, который имеет функцию доступа к беспроводной сети и соединяет подвижную сеть передачи данных с серверами приложений или другими подвижными терминалами.

3.1.10 подвижный пользователь (mobile user) [ITU-T X.1121]: Объект (человек), который применяет и эксплуатирует подвижный терминал для получения различных услуг от поставщиков прикладных услуг.

3.1.11 информация, позволяющая установить личность (personally identifiable information (PII)) [b-ITU-T Y.2720]: Любая информация, относящаяся к какому-либо живущему лицу, которая позволяет установить личность такого лица (в том числе информация, способствующая установлению личности лица, в сочетании с другой информацией, даже если эта информация не позволяет точно установить это лицо).

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации даны определения следующих терминов.

3.2.1 приложения, использующие идентификацию на основе маркеров (applications using tag-based identification): Приложения, которые состоят, как минимум, из следующих элементов: идентификатор, терминал получения ID, маркер ID и сеть (сети). В этом приложении идентификатор хранится на маркере ID и вся информация, касающаяся установления личности, предоставляется на стороне сети.

ПРИМЕЧАНИЕ. – Идентификатор хранится на маркере ID (или в маркере ID, в зависимости от вида маркера ID), и устройство ID считывает или списывает идентификатор из маркера ID с помощью оптического сканера (только чтение), фотокамеры (только чтение), IrDA (чтение/запись), радиочастотного устройства (чтение/запись) или другими аналогичными методами.

3.2.2 бизнес-для-потребителя (business-to-consumer B2C): Деловые взаимоотношения между предприятиями и потребителями, при которых поставщики услуг предоставляют ценные и полезные услуги потребителям, и потребители ими пользуются.

3.2.3 описание политики PII "по умолчанию" (default PII policy profile): Установленный набор правил защиты PII и принципов приложения, использующего идентификацию на основе маркеров.

3.2.4 идентификация (identification ID): Процедура установления конкретной личности объекта из большого числа объектов путем считывания идентификационных признаков с маркеров ID.

3.2.5 пользователь маркера ID (ID tag user): Лицо, которое приобретает и носит или использует объект с активным маркером ID.

3.2.6 пользователь терминала получения ID (ID terminal user): Лицо, которое пользуется или управляет терминалом получения ID. Типичным примером пользователя терминала получения ID мог бы быть подвижный пользователь с терминалом получения ID.

3.2.7 персонализированный маркер ID (personalized ID tag): Такой маркер ID, который содержит идентификатор, позволяющий точно установить личность, а не безымянный объект.

3.2.8 услуга защиты PII (PII protection service (PPS)): Услуга безопасности, которая обеспечивает защиту PII маркера ID и/или пользователей терминалом получения ID в приложении, использующем идентификацию на основе маркера ID. PPS управляет (т. е. создает/обновляет/ удаляет/исполняет) описанием правил PII пользователя (маркером ID и/или терминалом получения ID) в сети в процессе работы приложения, использующего идентификацию на основе маркеров.

3.2.9 краткое описание правил (PII policy profile): Установленный набор правил и принципов защиты PII.

3.2.10 определяемое пользователем краткое описание правил PII (user-defined PII policy profile): Установленный набор правил и принципов защиты PII, определенный пользователем (маркера ID и/или терминала получения ID).

4 Сокращения

В настоящей Рекомендации используются следующие сокращения:

ASP	Application Service Provider	Поставщик прикладных услуг
B2C	Business-to-Customer	Бизнес-для-потребителя
ID	Identification	Идентификация
IrDA	Infrared Data Association	Ассоциация передачи данных в инфракрасном диапазоне
OECD	Organization for Economic Cooperation and Development	Организация экономического сотрудничества и развития
PII	Personally Identifiable Information	Информация, позволяющая установить личность
PPS	PII Protection Service	Услуга защиты PII
RF	Radio Frequency	Радиочастота
RFID	Radio Frequency Identification	Радиочастотная идентификация
SCM	Supply Chain Management	Управление цепочкой поставок

5 Условные обозначения

Не имеется.

6 Общие положения

Широкое применение идентификационных маркеров, в том числе маркеров RFID, может вызвать обеспокоенность в отношении нарушения конфиденциальности из-за способности технологии RFID

выполнять функции автоматического сбора и обработки данных с возможным раскрытием таких данных неограниченному кругу лиц (преднамеренно или случайно).

Для приложений, использующих идентификацию на базе маркеров и основанных на маркере личной идентификации в персонализированных послепродажных приложениях управления, приложениях здравоохранения и т. д., вопрос обеспечения конфиденциальности становится серьезной проблемой.

В научных и промышленных кругах большая часть усилий в направлении механизма защиты PII сфокусирована на установлении правил аутентификации между маркером ID и терминалом получения ID. Заметим, однако, что эти усилия не могут применяться в реальных условиях эксплуатации, в частности к приложениям, использующим идентификацию на основе маркеров, в среде, где значимая информация для идентификации находится на сервере в сетевом домене. Таким образом, очень важно предложить пригодный механизм защиты PII в среде приложений, использующих идентификацию на основе маркеров. Механизм защиты PII на основе описания может стать одним из множества возможных решений в таких условиях.

В настоящей Рекомендации описан ряд нарушений информации, позволяющей установить личность (PII), для приложений, в которых используется идентификация на основе маркеров, и требования к защите PII, а также базовая структура защиты PII на основе краткого описания правил.

7 Приложения B2C, использующие идентификацию на основе маркеров

Приложение, использующее идентификацию на основе маркеров, определяется как расширенное приложение с более общей идентификацией, используемое для связи с рядом сетевых, межсетевых и глобальных прикладных систем. Другими словами, приложение, использующее идентификацию на основе маркеров, это приложение в глобальной сети, которое запускается маркером ID (включая RFID).

Приложения, использующие идентификацию на основе маркеров, уже широко применяются в таких отраслях, как управление цепочками поставок (SCM) и складской учет, а также в качестве мер предотвращения поставки фальсифицированных медикаментов. Приложение, использующее идентификацию на основе маркеров, теперь простирается до области конечного пользователя, например для доставки информационного контента, которая запускается маркером ID, послепродажное управление физическим объектом, записи историй болезни, контроль уплаты налогов и т. п., а также в промышленных приложениях.

Приложения B2C, использующие идентификацию на основе маркеров, могут быть разделены на три типа:

a) Потребителем является пользователь терминала получения ID: например, в службе доставки информационного контента потребитель получает информацию, используя терминал получения ID, которым он/она владеет. В этом виде службы поставщики большинства прикладных услуг могут предположить, что вероятно, этот терминал получения ID имеет возможность подвижной связи и возможность воспроизведения мультимедийной информации. На рисунке 1 показана базовая модель приложения этого типа, использующего идентификацию на основе маркеров. Она состоит из двух основных сетевых операций: распознавание ID и получение информации. Распознавание ID – это процедура передачи или распознавания идентификатора по адресу [b-ITU-T Y.2213]. Подвижный терминал, снабженный терминалом получения ID, сначала распознает идентификатор, полученный от маркера ID через справочную службу, а затем извлекает содержимое.

Рисунок 1 – Базовая модель приложения B2C, использующего идентификацию на основе маркеров

b) Потребителем является пользователь маркера ID: типичным примером такого приложения B2C, использующего идентификацию на основе маркера, являются операции по контролю доступа и/или установления личности, например проверка на входе, проверка паспорта, водительских прав, услуга послепродажного управления и т. д. В модели приложения данного типа терминалы получения ID относятся к фиксированному и/или подвижному типу устройств; потребителю может не понадобиться иметь свой собственный терминал.

c) Потребитель является и пользователем маркера ID, и пользователем терминала получения ID. В этой услуге получения информации о продукции (основной тип приложения B2C, использующего идентификацию на основе маркеров), потребитель, после приобретения маркированной продукции и после получения информации о продукции на свой подвижный терминал, становится также пользователем маркера. В другом примере, из области услуг здравоохранения, можно рассмотреть возможность маркирования медицинских карт маркером ID. В этом приложении пользователями маркера ID являются различные виды потребителей, например врач, пациент, медсестра и т. п. Пользователь маркера ID может просмотреть запись о своем пациенте, используя подвижный терминал со своим маркером ID, имеющий возможность считывать данные медицинской карты.

Поскольку многие приложения, использующие идентификацию на основе маркеров, расширяются, превращаясь в приложения B2C, потребители крайне озабочены утечкой PII через маркеры ID. В данной Рекомендации мы сосредоточили свои усилия, главным образом, на модели приложений B2C, использующих идентификацию на основе маркеров.

8 Эталонная модель приложений B2C, использующих идентификацию на основе маркеров

На рисунке 2 показана эталонная модель приложений B2C, использующих идентификацию на основе маркеров.

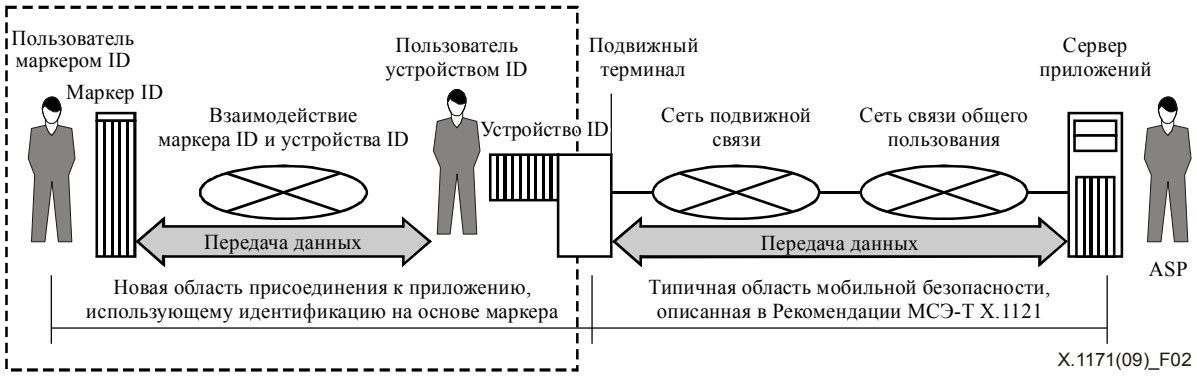

Рисунок 2 – Эталонная модель приложений B2C, использующих идентификацию на основе маркеров

Эта эталонная модель является расширенной моделью прямой связи между конечными пунктами в Рекомендации МСЭ-Т X.1121. Вновь добавленные элементы включают в себя маркер ID, пользователя маркера ID, взаимодействия маркера ID и устройства ID и устройства ID. В этой модели (подвижный) терминал может быть стационарным проводным терминалом, а также беспроводным подвижным терминалом, и может рассматриваться в качестве устройства ID.

9 Нарушение целостности PII в приложениях B2C, использующих идентификацию на основе маркеров

В условиях приложений, использующих идентификацию на основе маркеров, главные нарушения PII происходят, когда права владения продуктом или документом, имеющим маркер ID, передаются физическому лицу.

В условиях приложений, использующих идентификацию на основе маркеров, существует несколько методов хранения/чтения идентификатора, например (двумерный) штрих-код и оптический сканер или камера, пассивный маркер RFID ближнего поля и считыватель, пассивный маркер RFID дальнего поля и считыватель. В этом разделе описываются только общие утечки PII в приложениях, на базе B2C, использующих идентификацию на основе маркеров. Точнее, следующие угрозы в данной Рекомендации не описываются:

– Общие угрозы безопасности в приложениях, использующих идентификацию на основе маркеров. В этом разделе описываются только угрозы, относящиеся к PII в приложениях, использующих идентификацию на основе маркеров.

– Угрозы, определяемые методами хранения/чтения идентификатора. Например, в случае маркера RFID, злоумышленник может проследить местонахождение пользователя маркера ID на продукте с RFID меткой при помощи идентификатора метки RFID. В Дополнении I представлено подробное объяснение такого прослеживания местонахождения в среде RFID.

– Угрозы между маркером ID и терминалом получения ID. В этом разделе описываются только угрозы PII, относящиеся к сети.

9.1 Утечка информации, относящаяся к идентификатору

Злоумышленник может прочесть информацию с маркера ID, не зная пользователя маркера ID помеченного продукта. Сначала злоумышленник считывает идентификатор с маркера ID, находящегося у пользователя. Затем он/она распознает идентификатор и запрашивает службу справочника о местонахождении информации. И, наконец, злоумышленник запрашивает информацию, относящуюся к маркеру ID. Более того, если информация относится к такому виду информации, как информация по кредитной карте или по медицинской карте и т. п., то это может означать гораздо более серьезное нарушение PII пользователя метки ID. На рисунке 3 изображена кража PII при помощи утечки информации. В такой ситуации злоумышленник может получить как некоторое количество динамической информации, например время и место приобретения помеченного продукта, отслеживание информации о продукте и пр., так и некоторое количество статической информации, например название и описание продукта.

Такой вид кражи PII предотвращается при помощи удаления маркера ID или отключения функциональных возможностей маркера ID. Однако во многих приложениях, использующих идентификацию на основе маркеров, например в услугах персонализированного послепродажного управления, услугах, относящихся к здравоохранению, и. т. д., сохранение маркеров ID и их функциональных возможностей жизненно важно.

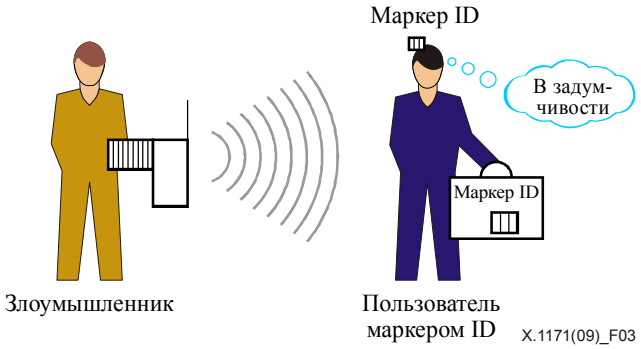

Рисунок 3 – Нарушение PII при помощи утечки информации

9.2 Утечка предыдущих контекстных данных

Злоумышленник может извлечь важные для пользователя данные, например предпочтения, привычки, области интересов и т. п., из данных предыдущего контекста, связанных с маркером ID. Кроме того, злоумышленник может использовать эти данные для незаконных или коммерческих целей без ведома пользователя. В такой ситуации повреждения пользователь обращается к пользователю терминала получения ID. Пользователь терминала получения ID считывает идентификатор с маркированных продуктов или документов при помощи своего терминала получения ID и получает полезную информацию от сервера приложений при помощи идентификации на основе маркеров. В этот момент данные регистрации разных ситуаций (дата проката фильма на DVD, дата и место приобретения объекта, место чтения плаката киноленты и пр.) могут собираться сетью приложений при помощи идентификации на основе маркеров; эти данные могут быть связаны с пользователем (см. рисунок 4).

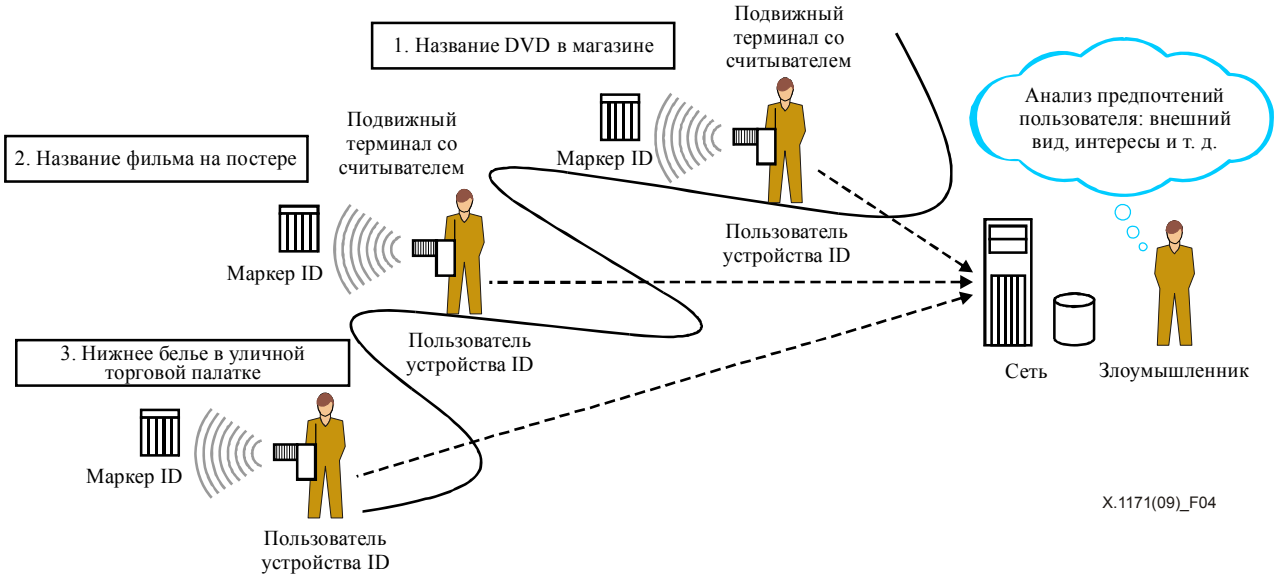

Рисунок 4 – Нарушение PII при помощи сбора исторических контекстных данных

9.3 Связь между нарушениями PII и эталонной моделью

Связь между нарушениями PII и объектами в модели, изображенной на рисунке 2, обобщена в таблице 1. В этой таблице колонки со знаком "X" означают, что нарушения PII в строке связаны с объектом или отношениям между объектами в колонке.

Таблица 1 – Связь между нарушениями PII и эталонной моделью

Объекты и отношения между объектами	**Нарушения**	
	Утечка информации из-за приложения(й), использующего(их) идентификацию на основе маркеров	**Утечка предыдущих контекстных данных, хранящихся на сервере(ах) приложений**
Связь между маркером ID и пользователем терминала получения ID		X
Связь между (подвижным) терминалом и сервером приложений	X	X
Связь между пользователем маркера ID и сервером приложений	X	
Связь между маркером ID и сервером приложений	X	
Сервер приложений	X	X

10 Требования защиты PII для приложений B2C, использующих идентификацию на основе маркеров

В этом разделе в основном описываются технические требования, работающие против двух нарушений PII, проанализированных в разделе 9. Более общие указания для пользователей и поставщиков RFID, относящиеся к защите PII в условиях технологии RFID, приводятся в других Рекомендациях. Эти требования частично основываются на принципах, взятых из указаний ОЭСР по защите конфиденциальности [b-OECD]. В Приложении A описываются принципы [b-OECD], рассматриваемые в этом пункте, а в Приложении B – другие принципы [b-OECD]. Следующие требования проистекают из наблюдений за нарушениями PII в приложениях B2C, использующих идентификацию на основе маркеров:

– управление PII пользователем маркеров ID и/или пользователем терминала получения ID;

– аутентификация для пользователя маркеров ID и/или пользователя терминала получения ID;

– управление доступом пользователя маркеров ID к PII в сервере приложений;
– конфиденциальность данных информации, связанной с маркером ID;
– согласие на сбор PII;
– технические средства защиты серверов приложений.

10.1 Управление информацией PII со стороны пользователя маркера ID и/или пользователя терминала получения ID

Необходимо, чтобы пользователь маркера ID и/или пользователь терминала получения ID могли управлять или обновлять информацию PII, связанную с его/ее маркером ID и/или терминалом получения ID по сети. Таким способом пользователь может определять, какую PII следует удалить или оставить в приложении, использующем идентификацию на основе маркеров. Кроме того, пользователь может определить крайний срок для его/ее PII в приложении, использующем идентификацию на основе маркеров.

10.2 Аутентификация пользователя маркеров ID и/или пользователя терминала получения ID

Сервер приложений, использующих идентификацию на основе маркеров, должен поддерживать процедуру аутентификации для пользователей маркеров ID, и если необходимо, сервер приложений может поддерживать процедуру аутентификации пользователя терминала получения ID (некоторые приложения, использующие идентификацию на основе маркеров, не требуют аутентификации пользователя).

10.3 Управление доступом пользователя маркеров ID к PII в сервере приложений

Доступ к PII пользователей маркеров ID, хранящейся в сервере приложений, должен быть защищен и ограничен разрешенными запрашивающими объектами, а также соответствующей информацией, необходимой каждому запрашивающему объекту.

10.4 Конфиденциальность данных информации, связанной с маркером ID

Сервер приложений, использующих идентификацию на основе маркеров, должен поддерживать конфиденциальность данных для обеспечения того, что информация, связанная с маркером ID, не будет прочитана неавторизованными пользователями.

10.5 Согласие на сбор PII

Сервер приложений, использующих идентификацию на основе маркеров, должен поддерживать процедуру согласия для сбора PII, в том числе данных регистрации, относящихся к пользователю терминала получения ID. Приложение, использующее идентификацию на основе маркеров, предоставляет техническое решение для поддержания PII в точном и обновленном состоянии, как того требует достижение определенной цели и ограничение соответствующей необходимой информацией. В процессе согласия это приложение должно удовлетворять цели сбора PII. Еще одно согласие пользователя необходимо в том случае, если ранее собранная PII будет использоваться для достижения другой цели, не предусмотренной в первоначальной цели.

10.6 Технические средства защиты серверов приложений

ASP приложений, использующих идентификацию на основе маркеров, отвечающий за обработку PII, должен принять технические меры защиты серверов приложений, включая PII.

10.7 Связь между требованиями и нарушениями PII

В таблице 2 приводятся общие данные о связи между требованиями защиты PII и нарушениями PII. В этой таблице ячейки со знаком "X" означают, что нарушения PII в колонке относятся к требованиям защиты PII в строке.

Таблица 2 – Связь между требованиями и нарушениями PII

Требования	Нарушения	
	Утечка информации, относящейся к идентификатору	**Утечка предыдущих контекстных данных**
Управление PII пользователем маркера ID и/или пользователем терминала получения ID	X	
Аутентификация для пользователя маркера ID и/или пользователя терминала получения ID	X	X
Управление доступом к PII пользователя маркера ID в сервере приложений	X	
Конфиденциальность данных информации, относящейся к маркеру ID	X	X
Согласие на сбор PII		X
Технические средства защиты серверов приложений	X	X

Приложение A

Основные принципы национального применения[2]

(Это Приложение является неотъемлемой частью данной Рекомендации)

- Ограничения в отношении сбора данных: Должны существовать ограничения в отношении сбора личных данных, и такие данные должны быть получены законным и честным путем и, в соответствующих случаях, с ведома или согласия субъекта данных.
- Качество данных: Личные данные должны иметь отношение к целям, для которых они используются, и, в такой мере, в какой это необходимо для достижения этих целей, они должны быть точными, полными и обновленными.
- Определение целей: Цели, для которых собираются личные данные, должны быть определены не позднее момента сбора данных, а их последующее использование должно быть ограничено достижением этих целей или других целей, которые совместимы с этими целями и которые должны определяться всякий раз, когда они изменяются.
- Ограничение использования: Личные данные не должны быть раскрыты, сделаны доступными или использованы каким-либо иным образом для целей, отличных от тех, которые были определены в соответствии с конкретной определенной целью.
- Гарантии безопасности: Личные данные должны быть защищены разумными гарантиями безопасности от таких рисков, как потеря данных или несанкционированный доступ к ним, уничтожение, использование, изменение или раскрытие данных.
- Прозрачность: Необходимо проводить общую политику, направленную на обеспечение прозрачности в том, что касается изменений, правил и стратегий в отношении личных данных. Должны быть обеспечены доступные средства для установления факта наличия или характера личных данных, основных целей их использования, а также идентичности контроллера данных и обычного места его деятельности.
- Участие физических лиц: любое физическое лицо должно иметь право:
  - a) получать у контроллера данных, или иным способом, подтверждение того, имеются ли у него относящиеся к нему данные или не имеются;
  - b) на то, чтобы относящиеся к нему данные были сообщены
    - в пределах разумного срока;
    - за умеренную плату, если плата вообще существует;
    - разумным образом;
    - а также в хорошо понятной ему форме;
  - c) получить объяснения причин возможного отказа в просьбе, сделанной в соответствии с пунктами a) и b), и иметь возможность оспорить такой отказ; и
  - d) оспорить относящиеся к нему данные и, в случае успеха, потребовать удаления, исправления, дополнения или изменения этих данных.
- Ответственность: Контроллер данных должен нести ответственность за соблюдение мер, приводящих в действие принципы, упомянутые выше.

---

[2] Эти принципы были взяты из части II "Указаний ОЭСР по защите конфиденциальности и потоков передачи личных данных за границу государства ", ОЭСР, 1980 год.

Приложение B[3]

Основные принципы международного применения: свободный поток информации и законные ограничения

(Это Приложение является неотъемлемой частью данной Рекомендации)

- Государства-Члены должны учитывать последствия для других Государств-Членов национальной обработки и реэкспорта личных данных.
- Государства-Члены должны принимать разумные и надлежащие меры для обеспечения того, чтобы трансграничные потоки личных данных, в том числе транзит через то или иное Государство-Член, были непрерывными и безопасными.
- Любое Государство-Член должно воздерживаться от ограничения трансграничных потоков личных данных между собой и другим Государством-Членом, за исключением случаев, когда последнее, по сути, еще не соблюдает настоящие указания или когда реэкспорт таких данных позволил бы обойти его национальное законодательство о защите частной сферы. Любое Государство-Член может ввести ограничения в отношении некоторых категорий личных данных, для которых его национальное законодательство о защите частной сферы предусматривает специальные правила, учитывающие характер этих данных, и для которых другое Государство-Член не предусматривает равноценной защиты.
- Государства-Члены должны воздерживаться от разработки законов, стратегий и процедур, под прикрытием защиты частной сферы и личных свобод, которые создавали бы препятствия для трансграничных потоков личных данных, выходя за рамки требований, присущих такой защите.

---

[3] Эти принципы были взяты из части III "Указаний ОЭСР по защите конфиденциальности и потоков передачи личных данных за границу государства ", ОЭСР, 1980 год.

Дополнение I

Отслеживание местоположения при помощи идентификатора в службах RFID

(Это Дополнение не является неотъемлемой частью данной Рекомендации)

Злоумышленник может отследить положение пользователя маркера ID помеченного продукта при помощи идентификатора маркера RFID. Этот вид нарушения безопасности позволяет отслеживать или наблюдать за определенным идентификатором маркера при помощи невидимого пиратского считывателя RFID. Так как злоумышленник может использовать идентификатор маркера в качестве личного идентификатора, он/она может с легкостью отследить местоположение пользователя, как это показано на рисунке I.1.

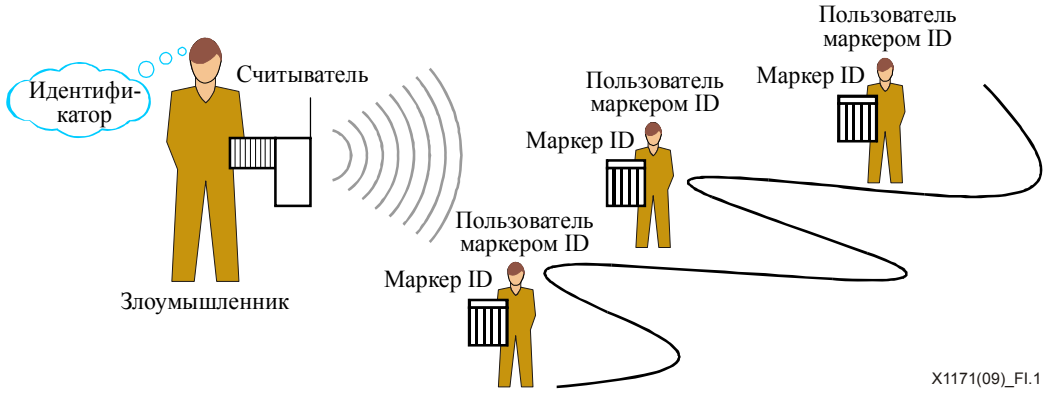

Рисунок I.1. – Угроза безопасности посредством отслеживания местоположения человека

Для защиты прослеживаемости идентификатора между маркером RFID и считывателем может применяться метод аутентификации. Маркер RFID открывает считывателю свой идентификатор, только если считыватель аутентифицирован маркером RFID. Другими словами, злоумышленник не может получить идентификатор маркера, не пройдя процедуру аутентификации. Однако если маркер RFID не имеет достаточно силы для работы с большим объемом вычислений, например криптографическое вычисление, этот метод аутентификации не может считаться реальным решением.

Другим решением может стать техника записи идентификатора. Запись идентификатора включает в себя периодическую запись идентификатора метки RFID с псевдоидентификатором или метаидентификатором; тем самым снижается возможность подключения идентификатора маркера ID и пользователя маркера ID. Тем не менее, следует заметить, что этот метод записи идентификатора не применим, если маркер RFID не имеет перезаписываемых функциональных возможностей или если маркер ID использует особый формат идентификатора (например, код EPC [b-EPCglobal]). Более того, эта техника неприменима к услугам, требующим быстрого чтения метки RFID, и может привнести излишнюю сложность в работу сервера.

Дополнение II

Услуга защиты PII (PPS) в приложениях, использующих идентификацию на основе маркеров

(Это Дополнение не является неотъемлемой частью данной Рекомендации)

II.1 Услуга защиты PII (PPS) в приложениях, использующих идентификацию на основе маркеров

PPS представляет собой один из примеров услуги защиты PII на основе описания правил PII пользователя.

В разделе II.3 описывается общий сценарий обслуживания PPS для приложений, использующих идентификацию на основе маркеров. Для PPS маркер ID или пользователь терминала получения ID, обслуживаемый специальным приложением, использующим идентификацию на основе маркеров, создает свои правила защиты PII для таких приложений и отправляет их доверенной системе третьей стороны (системе PPS). Затем эта система создает описание правил PII пользователя и оправляет его на серверы приложений (системы на стороне серверов). С этого момента серверы приложений могут управлять доступом к информации PII, связанной с маркером ID и/или пользователем терминалом получения ID.

II.2 Элементы услуги PPS в приложениях, использующих идентификацию на основе маркеров

PPS состоит из трех следующих объектов (см. рисунок II.1):

– Система PPS. В качестве объекта с функциями управления для правил PII пользователя, этот объект создает описание правил PII, определенных пользователем, для правил PII пользователя и предоставляет описание пользователя системе(ам) на стороне службы.

  ПРИМЕЧАНИЕ. – В случае централизованной системы PPS, которая отвечает за множество приложений, использующих идентификацию на основе маркеров, должны выполняться соответствующие контрмеры против отдельных случаев ошибки. Однако, в зависимости от случая применения, может существовать только одна система PPS для приложения, использующего идентификацию на основе маркеров.

– Система на стороне службы. Объект, который предоставляет информацию, связанную с идентификатором маркера ID, т. е. который может рассматриваться как сервер приложений, использующих идентификацию на основе маркеров. Поэтому на стороне службы может существовать множество систем для приложений, использующих идентификацию на основе маркеров. Этот объект выполняет функцию контроля доступа при помощи определенного пользователем описания правил PII или описания правил PII, используемого по умолчанию.

– Система на стороне пользователя. Объект с функциями беспроводного (или проводного) доступа к сети и, если это необходимо, идентификатором функции захвата, этот объект может быть подвижным терминалом с терминалом получения ID. Посредством такой системы на стороне пользователя маркер ID и/или пользователь терминала получения ID могут иметь доступ к системам PPS и к стороне службы. При помощи системы на стороне пользователя пользователь управляет своими правилами защиты PII в определенных приложениях, использующих идентификацию на основе маркеров.

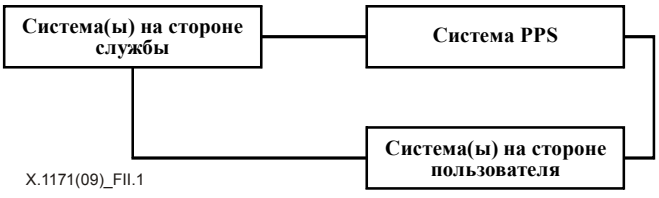

Рисунок II.1 – Элементы услуги PPS в приложениях, использующих идентификацию на основе маркеров

II.3 Общий сценарий услуги PPS

Сценарий услуги для PPS в основном происходит из процедуры персонализации маркера, например покупки помеченного продукта. На рисунке II.2 показан общий поток приложений, использующих идентификацию на основе маркеров.

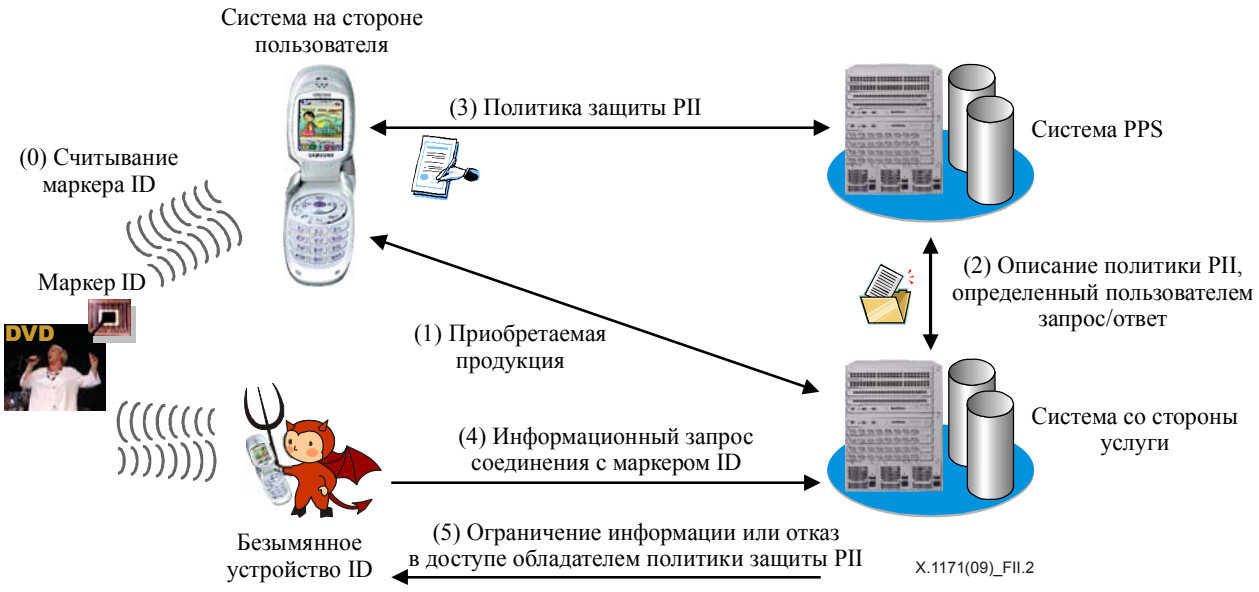

Рисунок II.2 – Основной алгоритм PPS

0) Покупатель считывает идентификатор помеченного продукта при помощи своего мобильного терминала, оборудованного терминалом получения ID.

1) Покупатель просматривает информацию, относящуюся к продукту, в служебной сети приложения и затем приобретает продукт при помощи одного из методов оплаты. С этого момента покупатель становится пользователем маркера ID.

2) Затем приложение, использующее идентификацию на основе маркеров, запрашивает у системы PPS определенное пользователем краткое описание правил PII, который затем передает приложению описание PII, определенное пользователем.

3) Система PPS получает правила защиты PII пользователя для этого приложения.

4) Кто угодно может запросить информацию, связанную с этим маркером ID, у системы на стороне службы.

5) Запрашивающий объект может просматривать всю информацию, предоставленную системой на стороне службы, если он является пользователем маркера ID. В противном случае запрашивающий объект получит или ограниченную информацию, или вообще не получит доступа.

ПРИМЕЧАНИЕ. – Необходимы дальнейшие работы для изучения сценариев разных случаев применения PPS для приложений, использующих идентификацию на основе маркеров, которые могут описывать преимущества PPS.

II.4 Функции PPS

Для удовлетворения требований защиты PII приложений, использующих идентификацию на основе маркеров, PPS использует следующие функции:

– управление кратким описанием правил PII;

– управление доступом;

– регистрация;

– передача краткого описания правил PII;

– обновление краткого описания правил PII.

II.4.1 Управление описанием правил PII

Управление описанием правил PII – это основная функция PPS. Система PPS управляет следующими двумя видами описаний правил PII:

– Описание правил PII, применяемое по умолчанию. Так называется форматированный набор правил и условий защиты PII приложений, использующих идентификацию на основе маркеров. Эти правила могут основываться на практиках честной информации, например описанных в Указаниях ОЭСР по защите конфиденциальности и потоков передачи личных данных за границу государства ([b-OECD]).
– Определенное пользователем описание правил PII. Так называется форматированный набор правил и условий защиты PII, определенных маркером ID и/или пользователем терминалом получения ID.

Система PPS выполняет функции создания и управления определенного пользователем или используемого по умолчанию описания правил PII. А именно, система PPS должна создать и управлять используемым по умолчанию описанием правил PII, для приложения, использующего идентификацию на основе маркеров, и определенным пользователем описания PII из правил защиты PII пользователя, как это определено в процедуре регистрации. Таким образом, это описание правил PII может быть передано системе(ам) на стороне служб. В основном оно может состоять из следующих пунктов:

– правила раскрытия для источников информации (включая PII);
– правила истечения срока для источников информации;
– правила сбора данных регистрации событий.

Затем система на стороне службы управляет доступом к источникам информации при помощи такого описания правил PII для всех, кто запрашивает информацию.

II.4.2 Управление доступом

Функция управления доступом системы PPS применяется для аутентификации идентичности пользователя или ASP и для авторизации доступа к источникам информации пользователя, которые, в основном, являются правилами защиты PII владельца.

ПРИМЕЧАНИЕ. – Использование слова "идентичность" производится с пониманием того, что в сфере связи это идентификатор или набор идентификаторов, которые подтверждены, что означает, что они были сочтены заслуживающими доверия в результате конкретной работы, произведенной частью сети, терминалом сети или пользователем после завершения процесса одобрения. В том смысле, в котором здесь используется этот термин, нельзя сделать вывод о том, что подтвержденные идентификаторы правильно установят личность.

С другой стороны, функции управления доступом системы на стороне службы – это важный элемент PPS, так как система на стороне службы должна управлять доступом ко всем источникам информации и поддерживать PII на основе определенного пользователем описания правил PII (или применяемого по умолчанию описания правил PII в отсутствие определенного пользователем описания правил PII). Система на стороне службы должна прослеживать, имеет ли запрашивающий доступ к PII определенного пользователя на основе определенного владельцем описания правил PII.

II.4.3 Регистрация

Система на стороне службы и система на стороне пользователя имеют процедуру регистрации с системой PPS. В процедуре регистрации информация о регистрации, предоставляемая системами на стороне службы и стороне пользователя, состоит из:

– Система на стороне службы. Информация об идентичности, включая информацию аутентификации, например пароль, и информацию о типе информации, т. е. информацию о цене, методе приобретения и т. д., представляемая системе на стороне пользователя сервером приложений, использующих идентификацию на основе маркеров;
– Система на стороне пользователя. Информации об идентичности, включая информацию аутентификации, например пароль, и информацию о собственных правилах защиты PII владельца и соответствующих приложениям, использующим идентификацию на основе маркеров.

Система PPS должна создавать используемое по умолчанию описание правил PII для системы на стороне службы и поддерживать применяемое по умолчанию описание правил PII для системы на стороне службы (см. рисунок II.3). Применяемое по умолчанию описание правил PII может создаваться при помощи функциональных возможностей управления описанием PII.

С другой стороны, система PPS должна создавать определенное пользователем описание безопасности PII на основе правил защиты PII пользователя. На рисунке II.3 показана процедура регистрации PPS.

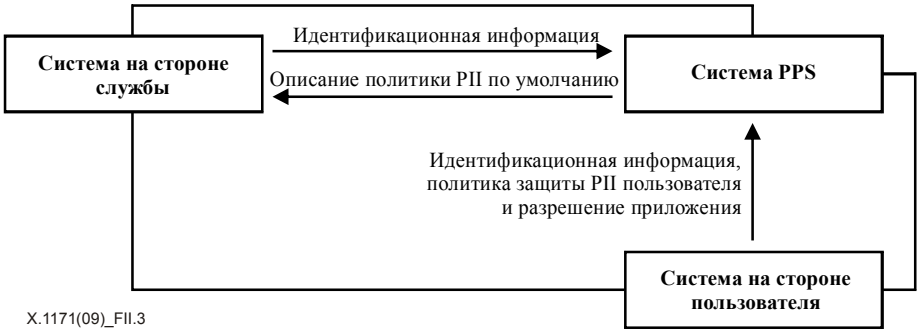

Рисунок II.3 – Процедура регистрации

II.4.4 Передача описания правил PII

Процедура передачи описания правил PII запускается системой на стороне службы. На рисунке II.4 показана процедура передачи описания PII.

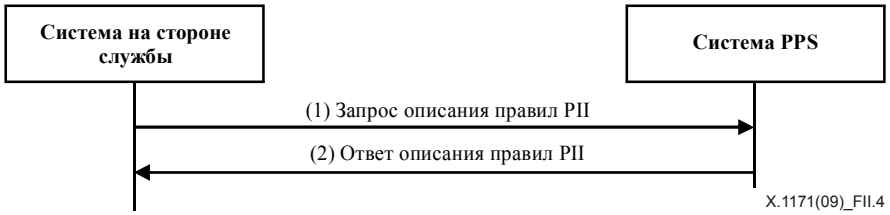

Рисунок II.4 – Процедура регистрации описания правил PII

1) Запрос описания правил PII. Система на стороне службы запрашивает определенное пользователем описание правил PII с идентичностью пользователя.

2) Ответ описания правил PII. Система PPS проверяет определенное пользователем описание правил PII для этого пользователя и отправляет определенное пользователем описание правил PII.

ПРИМЕЧАНИЕ. – Слово "идентичность" используется с пониманием того, что в сфере связи это идентификатор или набор идентификаторов, которые подтверждены, что означает, что они были сочтены заслуживающими доверия в результате конкретной работы, произведенной частью сети, терминалом сети или пользователем после завершения процесса одобрения. В том смысле, в котором здесь используется этот термин, нельзя сделать вывод о том, что подтвержденные идентификаторы правильно установят личность.

II.4.5 Обновление описания правил PII

Процедура обновления описания правил PII запускается системой PPS. Когда пользователь изменяет свои правила защиты PII, система PPS повторно создает определенное пользователем описание правил PII. Затем система PPS отправляет сообщение обновления описания правил PII всем системам на стороне службы, зарегистрированным в системе PPS. После этого каждая система на стороне службы обновляет определенное пользователем описание правил PII и отправляет сообщение ответа на обновление описания правил PII. На рисунке II.5 показана процедура обновления описания правил PII.

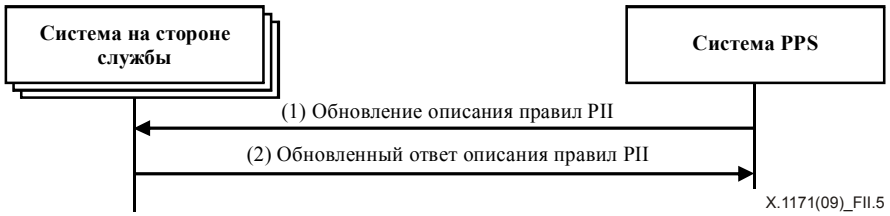

Рисунок II.5 – Процедура обновления описания политики PII

1) Обновление описания правил PII. Система PPS отправляет обновленное определенное пользователем описание PII каждой системе на стороне службы.

2) Ответ на обновление описания правил PII. Каждая система на стороне службы отправляет сообщения ответа на обновление системе PPS.

Библиография

[b-ITU-T F.771] Рекомендация МСЭ-Т F.771 (2008 г.), *Служебные описание и требования для доступа к информации мультимедиа, запускаемого идентификацией на основе маркирования*.

[b-ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.), *Архитектура безопасности для взаимосвязи в открытых системах для приложений CCITT*.

[b-ITU-T X.811] Рекомендация МСЭ-Т X.811 (1995 г.) | ISO/IEC 10181-2:1996, *Информационная технология – Взаимосвязь открытых систем – Инфраструктуры безопасности для открытых систем: Инфраструктура аутентификации*.

[b-ITU-T Y.2091] Рекомендация МСЭ-Т Y.2091 (2008 г.), *Термины и определения для сетей последующего поколения.*

[b-ITU-T Y.2213] Рекомендация МСЭ-Т Y.2213 (2008 г.), *Требования и качественные показатели для сетевых аспектов приложений и служб, использующих идентификацию на основе маркеров.*

[b-ITU-T Y.2720] Рекомендация МСЭ-Т Y.2720 (2009 г.) *Структура управления определением идентичности в СПП.*

[b-EPCglobal] EPCglobal standard (2008), EPCglobal Tag Data Standards Version 1.4. <http://www.epcglobalinc.org/standards/tds/tds_1_4-standard-20080611.pdf>

[b-OECD] ОЭСР (1980 г.), *Указания ОЭСР по защите конфиденциальности и потоков передачи личных данных за границу государства*. <http://www.oecdbookshop.org/oecd/display.asp?CID=&LANG=EN&SF1=DI&ST1=5LMQCR2K94S8>

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
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	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
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 и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2009 г.