Международный союз электросвязи

МСЭ-Т X.1275

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(12/2010)

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

Безопасность киберпространства – Управление определением идентичности

Руководящие указания по защите информации, позволяющей установить личность, при применении технологии RFID

Рекомендация МСЭ-Т X.1275

ITU-T

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.379
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
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
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

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

Рекомендация МСЭ-Т X.1275

Руководящие указания по защите информации, позволяющей установить личность, при применении технологии RFID

Резюме

В Рекомендации МСЭ-Т X.1275 отмечается, что технология радиочастотной идентификации (RFID) служит для представления информации, относящейся, в частности, к товарам, которые человек либо надевает на себя, либо носит с собой, и что при использовании этой технологии возможны злоупотребления. В то же время эта технология значительно упрощает доступ к такой информации и ее распространение в нужных целях. Злоупотребление может проявляться в виде отслеживания местоположения человека или в виде нарушения его или ее конфиденциальности каким-то другим незаконным способом. В связи с этим в настоящей Рекомендации приводятся руководящие указания в отношении процедур RFID, которые могут применяться для того, чтобы пользоваться преимуществами технологии RFID, прилагая при этом все усилия для защиты информации, позволяющей установить личность.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1275	17.12.2010 г.	17-я

Ключевые слова

Информация, позволяющая установить личность, приложение RFID.

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.1275

Руководящие указания по защите информации, позволяющей установить личность, при применении технологии RFID

1 Сфера применения

В настоящей Рекомендации содержатся руководящие указания для пользователей и поставщиков средств радиочастотной идентификации (RFID), включая поставщиков услуг и производителей RFID, в отношении защиты информации, позволяющей установить личность, в целях обеспечения конфиденциальности при использовании технологии RFID.

Эти руководящие указания могут применяться к случаям, в которых система RFID может использоваться для нарушения конфиденциальности личности; например, информация, позволяющая установить личность, записывается в маркер RFID, и в дальнейшем осуществляется ее сбор, или устанавливается связь информации об объекте, собираемой с использованием RFID, с информацией, позволяющей установить личность. Однако это не относится к случаям, когда сбор и использование информации об объекте осуществляется без какого-либо риска раскрытия информации, позволяющей установить личность, и нарушения конфиденциальности.

Настоящие руководящие указания направлены на защиту информации, позволяющей установить личность, в целях обеспечения конфиденциальности личности, которая теоретически может быть затронута системой RFID, а также на обеспечение безопасных условий использования RFID. Эти руководящие указания призваны стать основными правилами для поставщиков услуг RFID и руководством для поставщиков услуг, производителей и пользователей RFID в том, что касается конфиденциальности при использовании RFID, и они подчиняются местному и национальному законодательству.

2 Справочные документы

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

[ISO/IEC 18000] ISO/IEC 18000-6 (2004), *Information technology – Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 MHz.*

[ISO/IEC 19762-3] ISO/IEC 19762-3 (2005), *Information technology – Automatic identification and data capture (AIDC) techniques – Harmonized vocabulary – Part3: Radio frequency identification (RFID).*

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 информация, позволяющая установить личность (PII) (personally identifiable information (PII)) [ITU-T X.1171]: Информация, относящаяся к любому человеку, которая позволяет идентифицировать его личность (включая информацию, позволяющую идентифицировать человека, если она используется в сочетании с другой информацией, даже если эта информация не позволяет четко определить личность).

3.1.2 система радиочастотной идентификации (RFID) (RFID system) [ISO/IEC 19762-3]: Система автоматической идентификации и система ввода данных, состоящая из одного или нескольких считывающих/опросных устройств и одного или нескольких приемопередатчиков, в которых передача данных обеспечивается на основе индуцированных или излучаемых электромагнитных несущих, модулированных соответствующим образом.

3.1.3 маркер радиочастотной идентификации (RFID tag) [ISO/IEC 19762-3]: Любой приемопередатчик вместе с механизмом хранения информации, прикрепленные к объекту.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 согласие (consent): Предоставление соглашения, подразумевающего индивидуальное ограниченное соглашение, которым диспетчеру данных дается разрешение или запрет на сбор, передачу, использование, хранение, архивацию или удаление конкретной PII.

3.2.2 диспетчер данных (data controller): Любой объект, который осуществляет привязку информации об объекте, записанной на маркер RFID, к PII, либо запись PII на маркер RFID, либо сбор PII, записанной на маркер RFID.

3.2.3 субъект данных (data subject): Любой объект, который может быть идентифицирован по одному или нескольким фрагментам данных, относящихся к его или ее физическим, физиологическим, умственным, финансовым, культурным или социальным свойствам.

3.2.4 разрешение (opt-in): Явно выраженное согласие какого-либо лица, предоставляющее диспетчеру PII право осуществлять сбор, передачу, использование, хранение, архивацию или удаление конкретной PII с определенной целью.

3.2.5 запрет (opt-out): Использование каким-либо лицом права выбора посредством представления запроса о недопущении сбора, передачи, использования, хранения, архивации или удаления конкретных данных.

3.2.6 личные данные (personal data): См. термин "информация, позволяющая установить личность". Данный термин является синонимом термину "информация, позволяющая установить личность".

3.2.7 производитель средств радиочастотной идентификации (RFID) (RFID manufacturer): Любая организация, которая осуществляет производство и продажу чипов/маркеров RFID, или производство (в том числе, обработку и упаковку) и продажу объектов со встроенными или прикрепленными маркерами RFID.

3.2.8 поставщик услуг радиочастотной идентификации (RFID) (RFID service provider): Любой объект, который предлагает какую-либо услугу, основанную на применении объектов со встроенными или прикрепленными маркерами RFID.

3.2.9 пользователь (user): Любое лицо, которое осуществляет покупку какого-либо объекта со встроенными или прикрепленными маркерами RFID, или пользуется услугой, основанной на применении какого-либо объекта со встроенным или прикрепленным маркером RFID.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения:

AES	Advanced Encryption Standard	Усовершенствованный стандарт шифрования
NFC	Near Field Communication	Связь ближнего радиуса действия
PDA	Personal Digital Assistant	Персональный цифровой помощник
PIA	Privacy Impact Assessment	Анализ воздействия на конфиденциальность
PII	Personally Identifiable Information	Информация, позволяющая установить личность
RFID	Radio frequency identification	Радиочастотная идентификация

5 Условные обозначения

Отсутствуют.

6 Принципы конфиденциальности

Руководящие указания, описанные в настоящей Рекомендации, основаны на принципах конфиденциальности, которые определены в указанных ниже документах: [b-Council of Europe], [b-EC1], [b-EC2], [b-OECD], [b-UNHCR]. Эти принципы включают, в частности:

– Ограничение 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 в отношении 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.

– Меры обеспечения безопасности: Личные данные должны быть защищены с помощью разумных мер обеспечения безопасности от таких рисков, как потеря данных или несанкционированный доступ к ним, уничтожение, использование, изменение или раскрытие данных.

– Открытость: Необходимо проводить общую политику, направленную на обеспечение открытости, 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 диспетчера данных и обычного места его нахождения.

– Участие физических лиц: любое физическое лицо должно иметь право:

  a) получать у диспетчера данных или иным способом подтверждение того, имеются ли у диспетчера данные, относящиеся к этому лицу, 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) получать объяснения причин возможного отказа в ответ на запрос, сделанный в соответствии с пунктами a) и b), и иметь возможность оспаривать такой отказ; и

  d) оспаривать относящиеся к нему данные и, в случае успеха, требовать удаления, исправления, дополнения или изменения этих данных.

– Ответственность: Диспетчер данных должен нести ответственность за соблюдение мер, приводящих в действие принципы, упомянутые выше.

7 Угрозы и нарушения в отношении PII в RFID

Угрозы и нарушения в отношении PII в RFID связаны с характеристиками бесконтактной технологии RFID, уязвимостью беспроводной связи и возможностью сбора информации третьей стороной с использованием считывающего устройства RFID. В Дополнении II приводятся подробные характеристики технологии RFID.

Растущие возможности для нарушений в отношении PII, обусловленных внедрением RFID, связаны с тем, что информация, получаемая диспетчером данных от маркера RFID, может использоваться по всей сети, а не только в соответствии с национальным и региональным законодательством, нормативно-правовыми актами и стратегиями. Эта информация для вывода PII может быть искажена. В следующем подразделе дано описание основных угроз и нарушений в отношении PII, возникающих при использовании технологии RFID.

Отметим, однако, что встраивание механизмов обеспечения безопасности в существующий маркер RFID сопряжено с трудностями, связанными с ресурсами, которые могут использоваться в том или ином маркере, например электроэнергией, временем обработки, объемом памяти и т. д. В Дополнениях I и II приводится описание ограничений, характерных для технологии RFID, а также технических мер защиты, применяемых в системах RFID.

7.1 Незаметность сбора данных

Благодаря конкретным характеристикам технологии RFID, сбор данных может осуществляться без ведома субъекта данных. Находящиеся в маркере RFID данные могут быть считаны без прямой видимости, поскольку радиоволны проникают сквозь препятствия, например сумки или одежду, и любое лицо, обладающее считывающим устройством, может считать данные с маркера RFID. Кроме того, размеры как маркера RFID, так и считывающего устройства могут быть чрезвычайно малыми, и могут действовать, не проявляя каких-либо признаков их функционирования. Данная характеристика может быть одной из причин для нарушений в отношении PII, свойственных технологии RFID.

7.2 Составление представления

Доступ к информации, содержащейся на маркере RFID, который принадлежит субъекту данных или который он носит с собой, может раскрыть секретные аспекты, связанные с его или ее предпочтениями. В частности, выводы, которые можно сделать из данных с маркеров RFID субъекта данных, могут раскрыть информацию, требующую защиты. Кроме того, при использовании приложений на базе RFID, например электронных паспортов и электронного здравоохранения, может быть раскрыта информация, требующая большей защиты, например информация о национальности, биометрическая информация или медицинские карты, эта информация может использоваться для формирования справок о субъекте данных.

7.3 Отслеживание

Субъектов данных, у которых имеется при себе маркер RFID, можно отследить, поскольку любому маркеру RFID присваивается однозначный идентификатор.

Возможность отслеживания обеспечивается путем сбора или обработки данных о местоположении и времени, и может осуществляться либо спустя некоторое время с помощью данных, которые уже хранятся в базе данных, либо в реальном времени.

8 Приложения RFID

Технология RFID широко используется во многих приложениях, например в здравоохранении, транспорте и материально-техническом обеспечении, электронном правительстве и информационных услугах, предназначенных для розничных сетей и систем поставок. В таблице 1 показаны возможные угрозы в отношении PII, существующие в типовых приложениях, где используется технология RFID.

Таблица 1 – Типовые приложения RFID и возможные угрозы для PII

Область	Типовые приложения	Информация, содержащаяся на маркере RFID	Возможные угрозы PII
Система поставок	Управление запасами	Продукт	Отслеживание, составление представления о лицах, осуществляющих инвентаризацию
	Розничная торговля (например, супермаркет)	Продукт	Отслеживание, составление представления (после покупки товара)
Транспортное и материально-техническое обеспечение	Билеты на общественный транспорт	Идентификатор пользователя, информация о начислении платы и т. д.	Отслеживание, составление представления
	Плата за проезд по автодороге	Идентификатор пользователя, информация о начислении платы и т. д.	Отслеживание, составление представления
	Слежение за транспортными средствами	Продукт	Отслеживание, составление представления
	Управление контейнерными перевозками	Продукт	Отслеживание, составление представления о лицах, обрабатывающих контейнеры

Таблица 1 – Типовые приложения RFID и возможные угрозы для PII (*окончание*)

Область	Типовые приложения	Информация, содержащаяся на маркере RFID	Возможные угрозы PII
Здравоохранение	Слежение за пациентами	Идентификатор пациента, медицинская карта и т. д.	Отслеживание, составление представления, незаметный сбор данных (например, имплантат VeriChip)
	Недопущение врачебных ошибок	Идентификатор пациента, медицинская карта, назначенные лекарства и т. д.	Отслеживание, составление представления
	Отслеживание поставок крови и медикаментов в целях борьбы с подделками	Продукт	×
Электронное правительство	Электронный паспорт	Идентификатор человека, национальность, биометрические данные	Отслеживание, составление представления, подделка PII
Информационные услуги	Интеллектуальные доски объявлений	Продукт	×

Как показано в таблице 1, не все приложения RFID вызывают обеспокоенность, связанную с нарушениями в отношении PI, и не все приводят к возможным проблемам. Если приложение RFID не касается пользователя, например ряд приложений, относящихся к системе поставок, то такая обеспокоенность вряд ли возникнет.

Однако, если рабочие производят обработку контейнеров, например, для других приложений, относящихся к системе поставок, действия этих рабочих могут контролироваться с помощью маркеров RFID.

В следующих далее подразделах приведен ряд примеров приложений вместе со сценариями услуг, которые могут вызывать обеспокоенность, связанную с нарушениями в отношении PII.

При совместном использовании считывающих устройств RFID и других (например, мобильных) приложений возникает много отношений по связи, что может расширить возможности для отслеживания и составления представления.

8.1 Управление системой поставок

На данный момент технология RFID уже длительное время широко используется для управления системой поставок. К основным бизнес-приложениям в области управления системой поставок, где используется RFID, относятся управление запасами/имуществом, приложения для розничной торговли и т. д. Розничная торговля является наиболее характерной услугой на базе приложения RFID. На рисунке 1 приведен пример использования RFID в приложении для розничной торговли, который показывает, как происходит распространение маркеров RFID.

Приложения RFID для розничной торговли предоставляются производителем, который изготавливает маркер RFID, записывает на него информацию об объекте и прикрепляет маркер к объекту. В данном примере рассматриваемая организация розничной торговли является поставщиком услуг RFID, который продает пользователю какой-либо объект с прикрепленным к нему маркером RFID. В системе RFID, предназначенной для управления системой поставок, как правило, применяются пассивные маркеры, и для защиты PII, относящейся к субъекту данных, в них используется пароль деактивации маркера и т. д. В некоторых случаях, например в приложениях, рассчитанных на отдельные товары, для управления системой поставок часто требуются пассивные маркеры с большой дальностью связи даже для отдельных наименований товаров.

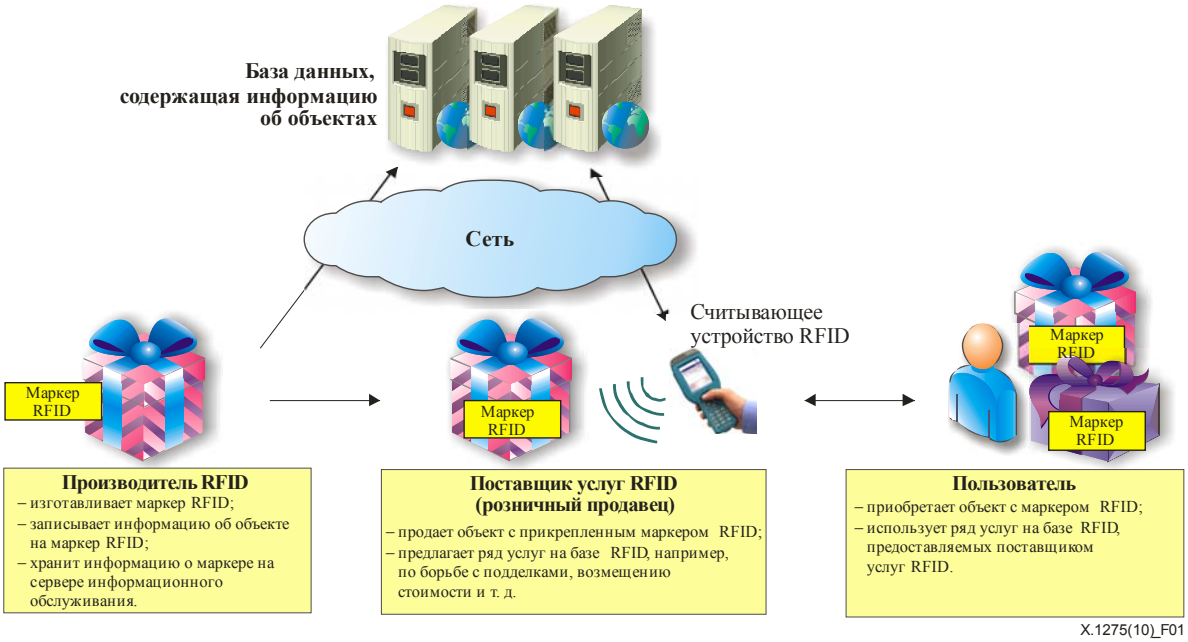

Рисунок 1 – Пример использования RFID в приложениях для розничной торговли

Что касается приложений для розничной торговли, обеспокоенность, связанная с нарушениями в отношении PII, возникает, главным образом, после того, как пользователь покупает объект, к которому прикреплен маркер RFID, поскольку участие пользователя происходит в месте совершения продажи только во время этого процесса. Когда пользователь покупает какой-либо объект с прикрепленным к нему маркером RFID, розничный продавец может определить предпочтения данного пользователя путем увязки информации об объекте, хранящейся на маркере RFID, с информацией о платеже пользователя или карточкой постоянного покупателя, а также с помощью постоянного наблюдения за характером покупательского поведения и его анализа. В этом случае поставщик услуг RFID становится диспетчером данных, а пользователь становится субъектом данных. При этом любое лицо, обладающее считывающим устройством, может считать маркер RFID, если только этот маркер не удален или уничтожен.

8.2 Транспортное и материально-техническое обеспечение

Системы RFID хорошо подходят для определенных приложений в области транспортного и материально-технического обеспечения. При условии надлежащего распределения считывающих устройств RFID, оборудованные маркерами автомобили можно отслеживать в пределах небольшой зоны, например склада или предприятия. Приложениями, которые могут дать повод для беспокойства в секторах транспортного и материально-технического обеспечения, являются системы продажи билетов на общественный транспорт и сбора платы за проезд по автодороге, как, например, системы, описанные в [b-E-ZPass].

В секторе транспортного и материально-технического обеспечения существует несколько приложений RFID. В частности, во многих системах продажи билетов на общественный транспорт и сбора платы за проезд по автодороге уже используется технология RFID. На рисунке 2 приведен пример приложения для транспортного обеспечения, показывающий, как маркер RFID используется в системе сбора платы за проезд по автодороге для идентификации и слежения за транспортными средствами.

В случае сбора платы за проезд по автодороге производитель RFID просто изготавливает маркеры RFID и продает их поставщику услуг RFID. В ряде конкретных случаев поставщик услуг RFID, который предоставляет услугу по сбору платы за проезд по автодороге и управляет этой услугой, может записать информацию о платеже пользователя на маркер RFID. Эта хранящаяся на маркере RFID информация относится к PII, которую можно использовать, для удобства идентификации пользователя.

Вместе с тем если информация о платеже пользователя связана с информацией, касающейся отслеживания перемещения пользователя, которая записана системой сбора платы за проезд по автодороге, то такая информация может представлять серьезную угрозу для PII пользователя. В этом случае поставщик услуг RFID, т. е. система сбора платы за проезд, становится диспетчером данных, а пользователь становится объектом данных.

Пассивные маркеры используются в основном в системах RFID, предназначенных для транспортного и материально-технического обеспечения. В транспортном обеспечении упрощенные криптографические схемы (на основе схемы симметричного шифрования) часто используются для проверки подлинности между маркером и считывающим устройством, а также для защиты дальнейшей передачи данных.

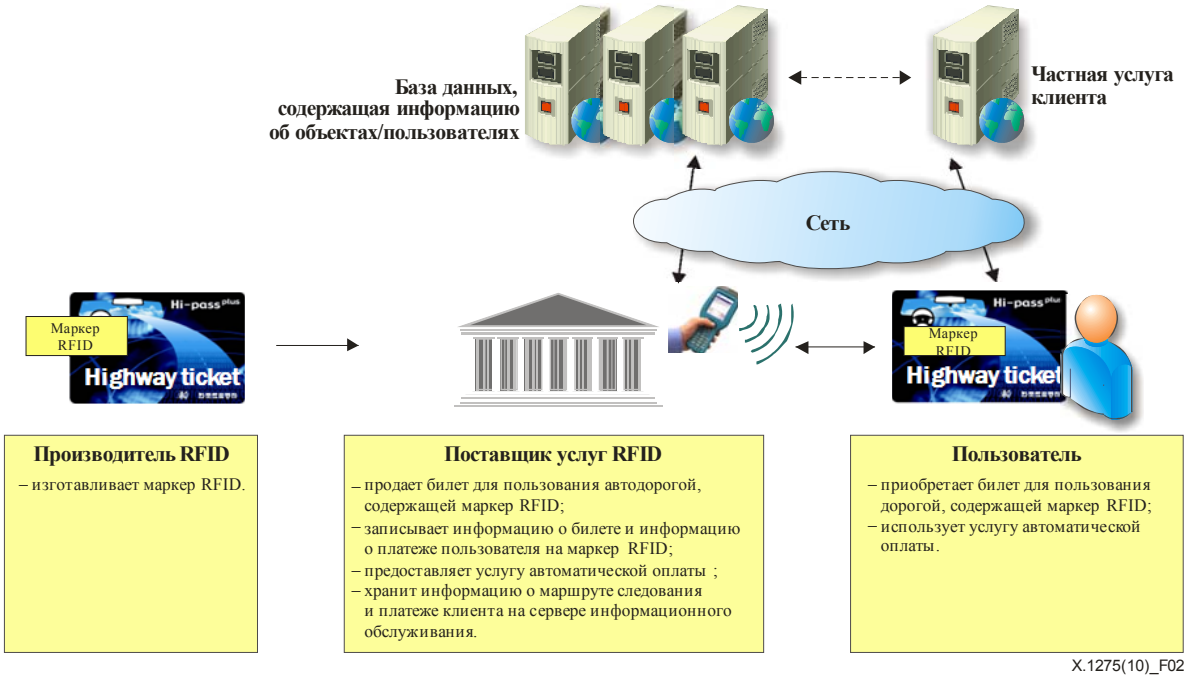

Рисунок 2 – Пример использования RFID для транспортного и материально-технического обеспечения

Что касается билетов на транспорт, то здесь часто используются бесконтактные смарт-карты со встроенными чипами RFID-маркером, которые работают на частотах ниже 13,56 МГц и имеют малую дальность связи. Если считывание осуществляется на небольшом расстоянии, как в данном случае, то использование обычных безопасных криптографических схем (даже ассиметричных схем), которые могут частично уменьшить риск утечки PII субъекта данных, является возможным, по крайней мере, технически. При этом следует отметить, что существующие протоколы, которые используются в настоящее время, способны только предотвращать копирование маркера, и таким образом, не допускать незаконного присвоения данных пользователя. Маркер ID до сих пор обнаруживается в незашифрованном виде в начале операции между маркером и считывающим устройством. Как таковой он может быть считан любым человеком, со всеми вытекающими отсюда проблемами, связанными с нарушениями в отношении PII. В любом случае данные, собранные в базе данных, когда пользователь взаимодействует с системой должны стать анонимными как можно скорее, для того чтобы уменьшить угрозу конфиденциальности пользователей.

8.3 Приложения в области здравоохранения и медицины

В здравоохранении также используется ряд приложений RFID. Однако использование RFID в приложениях здравоохранения может вызывать обеспокоенность возможными нарушениями в отношении PII, вследствие конфиденциального характера медицинских данных, требующих защиты. К приложениям здравоохранения на базе RFID относятся: слежение за пациентами для обеспечения их безопасности, осуществление мер по борьбе с подделкой медикаментов, обеспечение соблюдения пациентом врачебных предписаний, а также отслеживание поставок крови. Системы RFID уже нашли применение в фармацевтической отрасли, где они способствуют отслеживанию поставок медикаментов в целях борьбы с подделками и потерями от краж в процессе транспортировки. На рисунке 3 приведен пример приложения RFID в области здравоохранения, показывающий, как используется маркер RFID.

Для целей обеспечения соблюдения врачебных предписаний производитель RFID просто изготавливает маркер RFID и продает его. Поставщик услуг RFID, т. е. доктора и медсестры в больнице, могут стать диспетчерами данных, которые записывают и ведут медицинскую информацию пациента.

В изображенном на рисунке 3 приложении врачи и медсестры больницы могут проверять историю болезни пациента и назначенные ему предписания, считывая информацию с маркера RFID, который носит пациент, и в дальнейшем принимать надлежащие меры на основе имеющейся информации. С другой стороны, в приложении по слежению приема лекарств, можно легко раскрыть записанную в маркер информацию о лице, имеющем у себя те или иные лекарства за пределами больницы или аптеки; кроме того, из хранящейся на маркере RFID информации можно узнать болезнь пациента. Вследствие этого риск раскрытия личной информации, относящейся к субъекту данных, может быть выше, чем в случае приложения, описанного на рисунке 3. Таким образом, если медицинская информация пациента, хранящаяся на маркере RFID или во внутренней базе данных, защищается ненадлежащим образом, это может представлять прямую угрозу для PII субъекта данных.

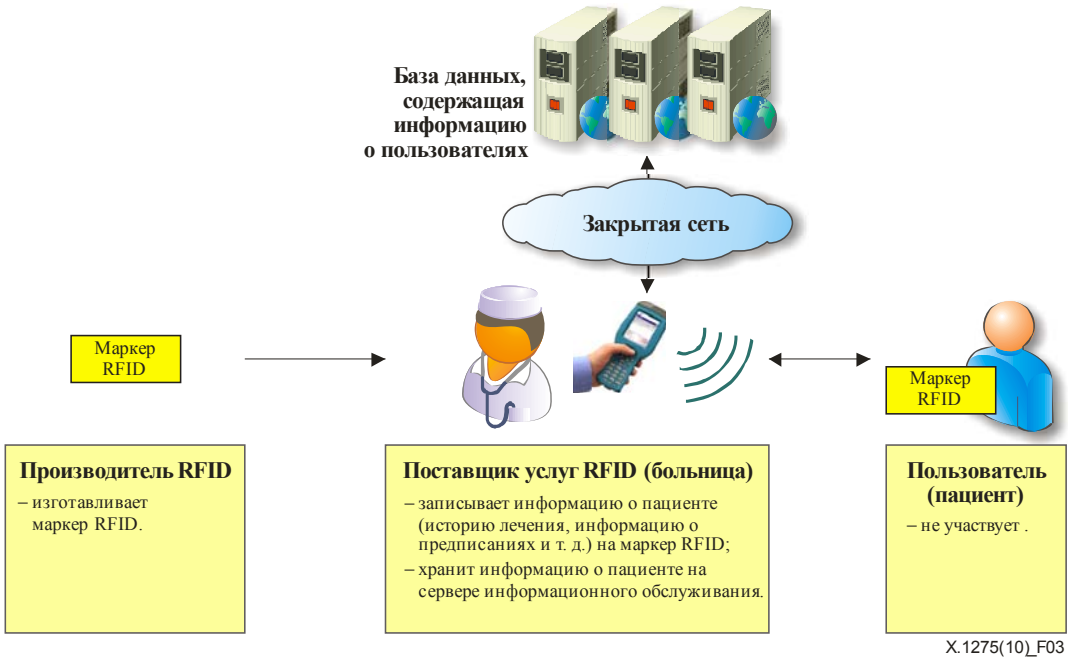

Рисунок 3 – Пример использования RFID в приложениях в области здравоохранения и медицины

Активные маркеры с большой дальностью связи, как правило, не используются в системах RFID, предназначенных для приложений в области здравоохранения и медицины. Однако имеются ситуации, в которых предпочтительно использовать активные маркеры с большой дальностью связи, например при уходе на дому для наблюдения за состоянием инвалида.

8.4 Электронное правительство

Электронный паспорт является наиболее типичным приложением в области электронного правительства. На встроенном в паспорт чипе RFID обычно содержится много PII субъекта данных, например номер паспорта, фамилия, национальность, фотография, биометрическая информация и т. д., тем самым, возможно, вызывая основную обеспокоенность, связанную с нарушениями в отношении PII.

Важно, чтобы маркер RFID сочетал в себе необходимые меры безопасности для снижения рисков сбора и копирования данных, содержащихся в электронном паспорте, поскольку эти данные относятся к разряду наиболее важной PII. На рисунке 4 приведен пример использования RFID в системе электронных паспортов и показано применение чипа RFID.

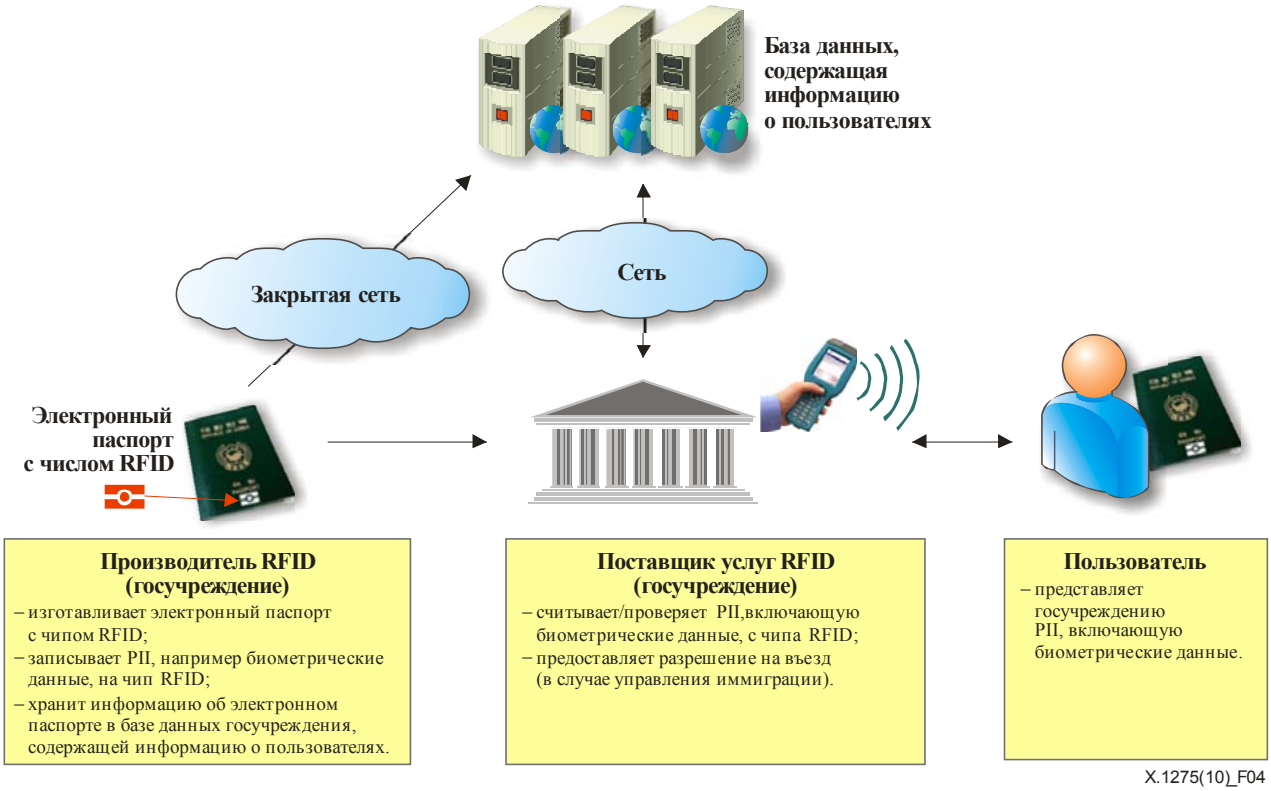

Рисунок 4 – Пример использования RFID в приложениях, связанных с применением электронных паспортов

Любой пользователь, желающий получить биометрический электронный паспорт, представляет PII, включая биометрические данные, государственным ведомствам, которые в случае приложения электронных паспортов могут являться производителями RFID. Эти органы изготавливают чип RFID и записывают на него PII пользователя, включая биометрические данные. Поставщик услуг RFID, например управление иммиграции, считывает PII с чипа RFID и проверяет эту информацию. Биометрические данные, хранящиеся на чипе RFID в системе электронных паспортов, относятся к PII, требующей наибольшей защиты; эта информация может использоваться для аутентификации или определения личности пользователя. Если эта информация окажется раскрыта или изменена, то такие биометрические данные поставят под большую угрозу конфиденциальность пользователя. В данном приложении и производитель RFID, и поставщик услуг RFID могут являться диспетчерами данных. Пользователь является субъектом данных. Как правило, в данном приложении используются пассивные маркеры с малой дальностью связи. В электронных паспортах должна обеспечиваться криптографическая защита.

Но иногда протоколы безопасности, описанные в стандартах, например [b-ICAO], являются необязательными или малоиспользуемыми. Таким образом, в области приложений, связанных с использованием электронных паспортов, все еще существует большая обеспокоенность в отношении конфиденциальности.

8.5 Информационные услуги

Интеллектуальная доска объявлений является одним из типовых приложений информационных услуг. Считывающим устройством RFID для интеллектуальной доски объявлений, как правило, оборудуется мобильное устройство, а маркер RFID остается в фиксированном положении. На рисунке 5 приведен пример использования RFID в приложении, связанном с применением электронной доски объявления, показывающий, как используются маркер и считывающее устройство RFID.

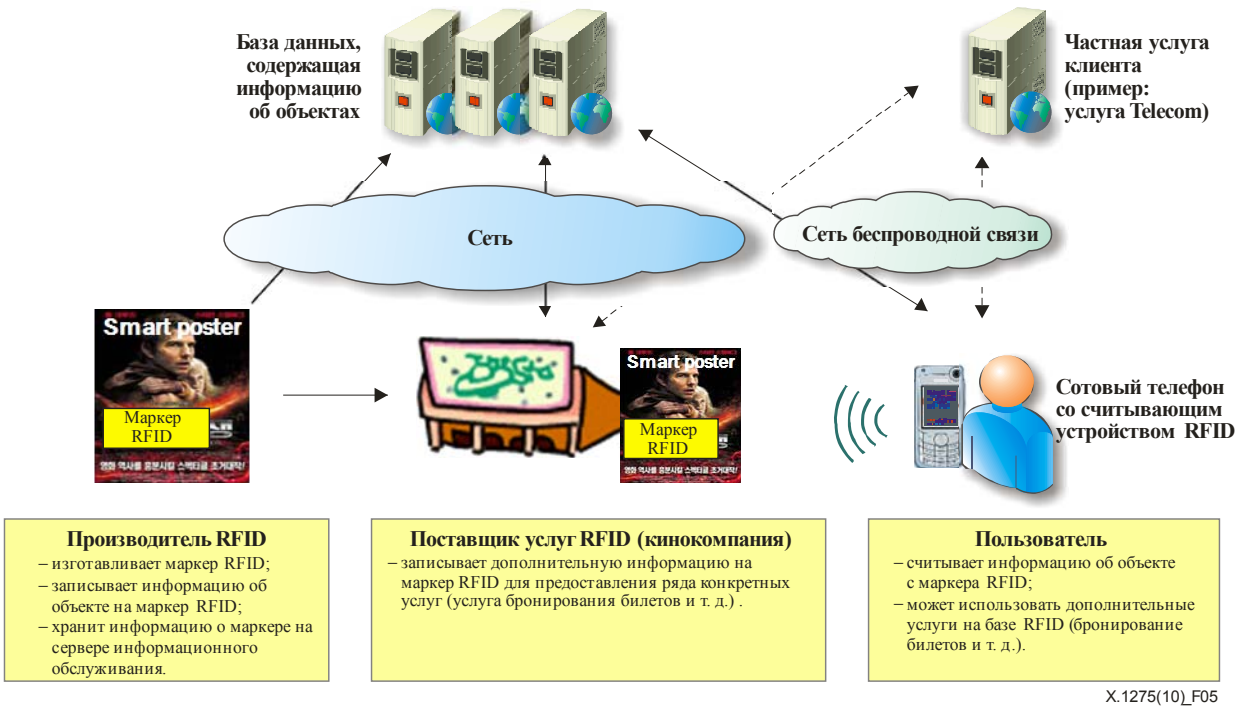

Рисунок 5 – Процесс использования RFID в приложении, связанном с применением интеллектуальной доски объявлений

Производитель интеллектуальной доски объявлений, использующей RFID, изготавливает чип RFID и продает его поставщику услуг RFID. Кинокомпания или театр являются поставщиками услуг RFID, которые записывают информацию о фильме на маркер RFID, встроенный в интеллектуальную доску объявлений. В других примерах информационных услуг дорожный атлас является той услугой, с помощью которой пользователю предоставляется информация о том, как проще всего отыскать нужный маршрут. Фактически, эти примеры приложений не вызывают обеспокоенности в отношении конфиденциальности, поскольку в них не используется личная информация или информация, требующая защиты. Вместе с тем следует отметить, что мобильность и радиус действия считывающего устройства RFID, встроенного в мобильное устройство, могут быть одним из факторов угрозы для конфиденциальности пользователей.

9 Руководящие указания по защите информации, позволяющей установить личность

Поскольку связанные с RFID технологии обеспечения конфиденциальности и защиты находятся на начальном этапе развития, даже с учетом их совершенствования, и, учитывая, что не существует универсального решения, так как условия использования и технические характеристики маркеров RFID в разных приложениях сильно различаются, применение этих технологий ко всей услуге RFID было бы преждевременным. Таким образом, эти руководящие указания сосредоточены, главным образом, на организационных мерах общего характера по защите PII субъекта данных, а не на технических мерах. Тем не менее следует принимать во внимание и технические меры: при разработке концепции приложения на базе RFID разработчикам предлагается рассматривать возможность применения современных технических решений, которые могут улучшить защиту конфиденциальности.

9.1 Правила и процедуры

Диспетчеры данных в услугах RFID должны формулировать правила и процедуры, регулирующие работу системы RFID, в частности надлежащее использование PII, и осуществлять их предварительную публикацию. В этих правилах и процедурах должны быть установлены роли и сферы ответственности, связанные с управлением PII и ее использованием. Кроме того, диспетчер данных должен возложить дополнительную ответственность на лицо, которое в отличие от других непосредственно осуществляет управление PII и ее использование.

9.2 Ограничения в отношении записи PII

Диспетчеры данных должны соблюдать принцип ограничения сбора данных. Следовательно, диспетчер должен обрабатывать только те данные, которые необходимы для цели применения этой системы, и PII не может храниться дольше, чем это необходимо.

В частности, диспетчеры данных в услугах RFID не должны осуществлять запись PII на маркеры RFID, за исключением случаев, когда запись PII предусмотрена законом или имеется явное письменное согласие субъекта данных.

Если диспетчеры данных должны записывать PII на маркере RFID, то вся PII, записанная на маркерах RFID, должна быть зашифрована. Если же диспетчерам данных необходимо получить согласие субъекта данных, то должно выбираться разрешение. Диспетчеры данных должны предварительно уведомить субъект данных о целях записи PII и возможности ее использования.

В услуге RFID диспетчеры данных должны получить индивидуальное, ограниченное согласие применительно к каждому записываемому элементу PII и должны информировать субъекты данных о целях записи или использования PII.

9.3 Информация, согласие, право доступа, исправление, право на возражение

Диспетчер данных должен соблюдать принцип индивидуального участия. Следовательно, в услуге RFID диспетчер данных обязан принимать надлежащие меры для предоставления пользователю информации о записанных сведениях PII и согласии, о праве на доступ, исправление и праве на отказ субъекта данных без каких-либо затрат для пользователя. Это применимо для PII, закодированной на маркере RFID, а также для PII, которая связана с информацией, хранящейся в маркерах RFID.

9.3.1 Информация

Субъект данных должен быть уведомлен диспетчером данных об обозначении, прикрепленного маркера RFID и установленных считывающих устройствах RFID, о третьих сторонах, которым данные были раскрыты, о любых исправлениях, удалениях или блокировках, если это не оказывается невозможным или не требует непропорциональное больших усилий.

9.3.1.1 Обозначение наличия прикрепленного маркера RFID

Применительно к встроенному или прикрепленному маркеру RFID, даже после того, как пользователь приобрел или получил объект, диспетчер данных в услуге RFID должен предварительно объяснить пользователю следующее, до того как он приобрел объект, или указать информацию на объекте, или использовать какие-либо легко заметные средства:

– тот факт, что имеется прикрепленный маркер RFID, а также его местоположение;
– характер и назначение маркера RFID;
– тип информации, записанной на маркере RFID;
– цель использования информации, записанной на маркере RFID;
– контактную информацию о лице, ответственном за защиту данных, в соответствии с пунктом 9.9.

Заметим, что если маркер не предназначен для использования субъектом данных, то, как только он приобрел объект, маркер должен быть деактивирован службой RFID или диспетчером данных в тот момент, когда пользователь покупает маркированный объект, если пользователь решит сохранить маркер в работе.

9.3.1.2 Обозначение установки считывающего устройства RFID

Любое лицо, устанавливающее считывающее устройство, которое способно считывать информацию объекта со встроенным или прикрепленным маркером RFID (или PII, записанную на маркер RFID и доставленную субъектам данных), должно указать, где и почему установлено считывающее устройство в таком месте, как контрольный пункт, так чтобы субъекты данных могли легко обнаружить это уведомление. Уведомление должно содержать, по крайней мере, идентичность оператора и контактные данные для лиц, желающих получить информацию о политике обслуживания.

Если считывающее устройство RFID встроено в персональный PDA или сотовый телефон, то дальность считывания при использовании считывающего устройства должна быть ограничена, с тем чтобы установить предел в отношении получения PII с маркера RFID.

9.3.2 Согласие

Диспетчер данных обязан заранее получить согласие субъекта данных. В розничной торговле и материально-техническом обеспечении, когда работает принцип деактивации по умолчанию, диспетчер данных может получить согласие субъекта данных в виде определенного письменного соглашения, регистрационной формы пользователя, электронной почты и т. д. В другом случае, таком как приложение биометрических электронных паспортов, согласия пользователя не требуется, потому что существует правовое обязательство собрать PII и сохранить ее в маркере.

9.3.3 Право доступа, исправление и право на возражение

Субъект данных должен иметь возможность получить от диспетчера данных, без ограничения через разумные промежутки времени и без чрезмерной задержки или затрат:

– подтверждение того, обрабатываются ли данные, касающиеся субъекта данных, и информация, касающаяся, по крайней мере, целей обработки, категорий рассматриваемых данных, а также получателей или категорий получателей, которым данные были раскрыты;

– сообщение субъекту данных в понятной форме данных, подвергающихся обработке и любой доступной информации относительно их источника;

– сведения о логике, применяемой в любой автоматической обработке данных, касающейся субъекта данных, по крайней мере, в случае автоматизированных решений.

Кроме того, диспетчеры данных в услуге RFID должны принять соответствующие меры к тому, чтобы обеспечить пользователя каким-либо методом коррекции, изменения и разрушения субъектов данных PII, бесплатно для пользователя.

Это применимо к PII, закодированной в маркерах RFID, а также к PII, которая связана с информацией, хранимой в маркерах RFID.

В частности, если маркер не используется для субъекта данных (например, в секторе розничной торговли, когда пользователь покупает маркированный объект), диспетчеры данных обязаны деактивировать, удалить или разрушить маркер, как это описано в пункте 9.5, если субъекты данных не просят, чтобы такой маркер остался в эксплуатации.

9.4 Ограничение в отношении сбора и привязки PII

Диспетчеры данных в услуге RFID должны уведомить соответствующий субъект данных, когда они собирают PII, записанную на маркере или сохраняют ее в базе данных с помощью привязки к объекту информации на маркере. Если поставщикам услуг RFID необходимо использовать PII для целей, отличных от тех, для которых она предназначалась, или необходимо предоставить данную информацию третьей стороне, то они должны предварительно получить определенное и обоснование письменное согласие субъекта данных.

9.4.1 PII, записанная на маркере RFID

Диспетчеры данных в услуге RFID должны надлежащим образом уведомить соответствующего субъекта данных или указать заметным образом тот факт, что они выполняют сбор PII, записанной на маркере RFID, а также заранее получить определенное и обоснованное согласие пользователя.

Когда диспетчеры данных собирают PII, они должны принять определенные меры по сертификации считывающего устройства и маркера RFID, например использовать между маркером и считывающим устройством RFID, а также между считывающим устройством и внутренней базой данных протоколы аутентификации. В настоящем документе под мерами по сертификации понимается криптографическая схема, используемая сервером внутренней базы данных, где хранится идентификатор маркера RFID и PII, для идентификации и аутентификации считывающего устройств RFID и диспетчера данных.

Однако для защиты PII следует отметить, что существующие протоколы аутентификации, используемые между маркером и считывающим устройством, эффективны только в том случае, если на маркере хранится дополнительная информация, помимо идентификатора маркера, такая как протоколы передачи существующего RFID, поскольку сам по себе идентификатор маркера не требует защиты.

9.4.2 Информация об объекте на маркере RFID, связанном с PII

Если диспетчеры данных хотят осуществить привязку записанной на маркере RFID информации об объекте к PII, то они должны предварительно уведомить соответствующего субъекта данных, указать на это заметным образом, а также получить определенное письменное и обоснованное согласие. При осуществлении диспетчерами данных привязки информации об объекте, записанной на маркере RFID, к PII, они должны принять определенные меры по сертификации считывающего устройства RFID, например использовать пароль или протоколы аутентификации между считывающим устройством и маркером RFID.

Если не предполагается связывать PII с информацией об объекте в момент ее сбора, однако это потребуется сделать впоследствии, то диспетчер данных должен уведомить пользователя о целях такого сбора и получить дополнительное и обоснованное согласие, для того чтобы выполнить законные требования.

9.5 Деактивация маркера RFID, когда цель достигнута

Встроенные или прикрепленные маркеры RFID должны быть устранены, уничтожены или окончательно деактивированы поставщиком услуги RFID или диспетчером данных в тот момент, когда пользователь приобрел или получил маркированный объект (в пункте продажи), за исключением случаев, когда пользователь решит сохранить маркер в работе или правовые или регуляторные требования указаний предписывают, чтобы маркер оставался активным. Даже если пользователь решит сохранить маркер в работе, диспетчер данных должен предоставить меры для устранения, уничтожения или окончательной деактивации маркеров на более позднем этапе по требованию субъекта данных. Пользователь должен быть уведомлен о последствиях деактивации.

Деактивация должна считаться нормальным случаем, но не для каждого приложения она может быть подходящим решением. Например, при деактивации маркера, который используется в приложении в области здравоохранения для доступа к истории болезни пациента и информации о назначенных предписаниях, продолжительное лечение пациента может быть затруднено. Деактивация может быть принудительной в приложениях, относящихся к управлению системой поставок, тогда как в приложениях транспортного и материально-технического обеспечения она может являться выбором пользователя. В случае приложений в сфере здравоохранения и электронного правительства деактивация не применяется для общественного здравоохранения или согласно закону. Производитель RFID или диспетчер данных в услуге RFID может использовать некоторые технические меры для деактивации RFID, такие как пароль деактивации, RFID Zapper и т. д. Однако, если деактивация маркера RFID ослабляет интерес пользователя или общественный интерес, диспетчер данных должны объяснить пользователю причину, или обозначить ее на объекте, или использовать легко заметные средства.

9.6 Информация о поставщиках услуг и диспетчерах данных

Поставщики услуг и диспетчеры данных должны разработать и опубликовать четкую, точную и легкую для понимания информационную политику для каждого приложения. Эта политика должна включать, по меньшей мере:

– идентичность и адрес диспетчеров;

– цель системы RFID;

– в частности, если будут обрабатываться персональные данные, то какие из этих данных должны быть обработаны системой и будет ли контролироваться местоположение маркеров;

– резюме оценки воздействия на конфиденциальность и защиту данных;

– вероятные риски конфиденциальности, если такие существуют, относительно использования маркеров в приложении, а также меры, которые люди могут принять, для того чтобы смягчить эти риски.

9.7 Организационные и технические меры по защите PII

– Когда диспетчеры данных службы RFID используют систему RFID для записи и сбора PII или привязки записанной на маркере RFID информации об объекте к PII, то для защиты PII в системе RFID они должны принимать организационные и технические меры безопасности, чтобы не допустить потери, кражи, утечки, изменения или повреждения соответствующей PII. Организационные и оперативные меры по защите PII включают следующее:

  • план по управлению внутренней безопасностью;

- анализ рисков, анализ угроз конфиденциальности и оценка воздействия на конфиденциальность;
- обучение по вопросам обеспечения конфиденциальности услуги RFID и т. д.

– Технические меры по защите PII включают следующее:
  - управление доступом и контроль доступа к внутренней базе данных;
  - управление доступом, для того чтобы предотвратить доступ к информации, хранящейся на маркере любого считывающего устройства;
  - шифрование PII, хранящейся на маркере и внутренней базе данных;
  - использование любого доступного протокола между считывающим устройством и маркером для защиты PII при передаче, например криптографические протоколы или любые методы, которые могут быть применимы;
  - использование маркеров, реализующих идентификаторы случайных маркеров для уменьшения рисков отслеживания;
  - сертификация действительного считывающего устройства RFID;
  - деактивация маркера RFID, например, с паролем деактивации маркера, RFID Zapper и т. д.;
  - ограничение возможности считывающего устройства и маркера, например создание активных помех, обнаружение датчика RFID, использование усеченных и блокирующих маркеров и т. д. [b-Juels];
  - меры по безопасности для смягчения рисков конфиденциальности, полученных от PIA.

Отметим, что организационные и технические меры для защиты PII, перечисленные выше, являются лишь частью всех мер. В будущем могут появиться новые меры, так как исследования в этой области продолжаются.

9.8 Оценка воздействия на конфиденциальность системы RFID

Когда поставщики услуг RFID и диспетчеры данных используют систему RFID для записи и сбора PII или привязки информации об объекте, записанной на маркере RFID, к PII, они должны принять меры по обеспечению того, чтобы в отношении PII не допускалось нарушений, проводя анализ и оценку любой возможности утечки PII или угроз PII, связанных с использованием системы RFID до того, как она будет внедрена, и теоретически – на этапе ее разработки.

Вследствие большого количества технических конфигураций и сценариев использования, не существует универсального решения, удовлетворяющего всем приложениям RFID. В связи с этим оценка воздействия на конфиденциальность могла бы помочь определить последствия для конфиденциальности (в соответствии с различными точками зрения, например правовые и технические аспекты), а также помочь отыскать наилучшие стратегии по смягчению этих последствий. Ниже приводится описание возможного процесса оценки воздействия на конфиденциальность (PIA). PIA должна охватывать всю систему RFID.

– Шаг 1: Начало реализации проекта.

  На данном шаге определяется масштаб коммерческого применения PIA, организуется группа по выполнению PIA и применяются средства PIA для отражения определенного масштаба.

– Шаг 2: Анализ потоков данных.

  Задача на данном шаге – построить диаграмму или блок-схему прохождения информации, позволяющей установить личность, таким образом, чтобы цель анализа рисков можно было проверить путем идентификации информации, позволяющей установить личность, которая обрабатывается целевой услугой оценки воздействия, и информационных ресурсов, которые содержат такую информацию.

  В частности, на данном шаге с помощью диаграммы или блок-схемы определяется, какая PII собирается, используется, хранится, удаляется или предоставляется третьей стороне, и какой для этого применяется метод. Кроме того, на данном шаге приводится описание роли и ответственности лиц, ответственных за каждый этап (сбор, использование, хранение и удаление) обработки PII.

– Шаг 3: Анализ факторов и рисков, связанных с нарушением в отношении информации, позволяющей установить личность.

  На данном шаге определяются угрозы и уязвимости применительно к ресурсам обработки информации, позволяющей установить личность, и выполняется анализ рисков в отношении таких ресурсов.

– Шаг 4: Составление плана оптимизации и планирование управления рисками.

  На данном шаге среди различных рисков, которые выявлены на этапе анализа рисков, связанных с PII, определяется уровень риска, который требует управления, а также разрабатываются методы управления для каждого риска, который нуждается в смягчении последствий и управлении.

– Шаг 5: Представление отчета о результатах PIA.

  На этом шаге, являющемся одним из важнейших шагов в процессе PIA, осуществляется составление и представление отчетов о процессе PIA и его результатах.

  В отчеты о PIA должны включать содержательные результаты обсуждения на всех этапах процесса PIA, от результатов PIA до контроля и управления рисками применительно к выявленному риску, связанному с личной информацией.

Отметим, что описанный выше процесс PIA является только иллюстрацией, а настоящий процесс PIA может быть адаптирован к конкретным потребностям или основываться на других существующих внешних процессах PIA.

9.9 Назначение официального лица, отвечающего за защиту данных

Диспетчеры данных должны назначить официальное лицо, отвечающее за защиту данных, в частности, за сохранение регистра, содержащего подробную информацию относительно операций по обработке, выполненную диспетчером данных, включая информацию об оценках воздействия на конфиденциальность и меры по безопасности приложений RFID, а также для того, чтобы незамедлительно обработать жалобы пользователей или запросы на осуществление их прав.

Дополнение I

Характеристики маркеров RFID и связанные с ними ограничения

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Классификация и характеристики маркеров RFID

В данном разделе описаны характеристики, используемые для классификации маркеров RFID, а также, почему методы обеспечения безопасности не могут свободно применяться к пассивным маркерам. Как правило, маркеры RFID делят на пассивные и активные. В таблице I.1 показана классификация маркеров.

Таблица I.1 – Классификация и характеристики маркеров RFID

Характеристики	Пассивные маркеры	Активные маркеры
Источник питания	Мощность передается от считывающего устройства	Внутренняя батарея
Дальность связи	3 м или меньше	100 м или больше
Срок использования	Не ограничен	Ограничен сроком использования батареи
Хранение данных	Малый объем памяти для чтения/ записи данных (несколько байт)	Большой объем памяти для чтения/записи данных (несколько кбайт)
Типовые применения	Управление запасами, розничная торговля, управление багажом/погрузчиками, карточки-пропуска и т. д.	Комплексные приложения, связанные со слежением за людьми и т. д. (здравоохранение или мониторинг зоны, системы сбора платы за проезд и т. д.)

Пассивные маркеры не имеют внутреннего источника питания; для передачи сигнала считывающему устройству в них используется мощность сигнала, передаваемого считывающим устройством. Дальность связи пассивных маркеров составляет порядка 3 метров и меньше. В случае работы на частоте 13,56 МГц, дальность связи составляет порядка 4~10 см, однако при использовании больших антенн она может быть увеличена приблизительно до 70 см. Маркеры, работающие в диапазоне УВЧ, имеют более высокую дальность связи, составляющую порядка 3~7 м.

В отличие от пассивных маркеров, активные маркеры имеют собственный источник питания, который позволяет им передавать сигнал считывающему устройству. Дальность связи активных маркеров составляет порядка 100 м и больше, однако срок использования ограничен сроком использования их батарей. Кроме того, активные маркеры являются более крупными и дорогими, чем пассивные.

Как правило, любая система, работающая в диапазонах низких (125/135 кГц) или высоких (13,56 МГц) частот, является пассивной системой. Системы, работающие в диапазоне ультравысоких частот (433/900 МГц; 2,45 ГГц) и диапазоне СВЧ, могут являться либо пассивными, либо активными.

В связи с малой дальностью сканирования, маркеры, работающие в диапазоне низких частот, используются в основном в области безопасности, управления имуществом, а также проверки аутентичности продукции. В то же время при предоставлении железнодорожных услуг и в области материально-технического обеспечения и распространения используются высокочастотные маркеры, поскольку дальность сканирования составляет 30 метров и более. В частности, маркеры с частотой 13,56 МГц встраиваются в кредитные карты или карты оплаты проезда в транспорте, и используются в них. Другими примерами приложений, в которых используется маркеры на частоте 13,56 МГц, являются электронный паспорт и беспроводная связь ближнего радиуса действия (NFC).

I.2 Ограничения, касающиеся пассивных маркеров

Многие эксперты, работающие в области RFID, отмечают, что цена маркера RFID должна быть ниже 5 центов, с тем чтобы способствовать развитию рынка RFID. Данное требование к цене маркера ограничивает выбор ресурсов, которые могут использоваться в маркере, например источника питания, времени обработки, объема памяти и количества логических элементов.

При стоимости маркера менее 5 центов, они смогут иметь память объемом не более сотни бит, 5–10 тысяч логических элементов и максимальную дальность связи в несколько метров. При таком порядке числа логических элементов для выполнения функций безопасности могут быть отведены лишь 250–3000 логических элементов. Кроме того, следует принять во внимание ограничения по мощности, поскольку большинство маркеров, используемых в настоящее время, относится к пассивным маркерам.

Мощность излучения считывающих устройств нередко ограничивается на законодательном уровне, и тем самым ограничивается мощность питания маркеров. При современном уровне развития технологии даже без ограничения затрат, использование в пассивных маркерах стандартных криптографических схем, обеспечивающих высокую защищенность, ограничивается маркерами ближнего радиуса действия. В маркерах, радиус действия которых составляет несколько метров, мощность считывающего устройства недостаточна для питания большого числа логических элементов, необходимых для реализации криптографических функций, обеспечивающих высокую защищенность.

В соответствии с [b-CRYPTREC] для реализации алгоритма асимметричного шифрования требуется приблизительно 6~13 тысяч логических элементов, и аналогичное количество элементов необходимо для реализации хеш-функции. Например, для стандартной реализации улучшенного стандарта шифрования (AES) требуется порядка 20~30 тысяч логических элементов. В настоящее время разрабатываются упрощенные алгоритмы шифрования, предназначенные для применения в маркерах RFID. Однако до сих пор возможность реализации алгоритма шифрования в маркере полностью не обеспечена вследствие этих ограничений в ресурсах.

Дополнение II

Технические меры для защиты PII в системе RFID

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Для того чтобы свести к минимуму угрозу нарушения конфиденциальности в прикладных услугах RFID, разрабатываются различные технологии защиты PII. В частности, разрабатываются новые технологии, которые описаны ниже, поскольку существующая технология шифрования и аутентификации, предназначенная для защиты конфиденциальности, не может применяться из-за ограничения ресурсов, используемых в маркерах RFID.

II.1 Деактивация маркера с использованием пароля

В данном наиболее распространенным методе защиты конфиденциальности пользователя используется то обстоятельство, что маркер RFID может быть в выключенном или активном состояниях. При необходимости считывающее устройство передает команду деактивации маркера, представляющую собой пароль (32 бита). Однако отключение маркера может использоваться только в некоторых приложениях, поскольку после применения команды отключения не сможет использоваться функция автоматической идентификации, которая является сильной стороной технологии RFID. Например, если при покупке отключить функцию маркера RFID, который прикреплен к изделию, то может оказаться невозможным вернуть изделие или возместить его стоимость, так как станет невозможным восстановить последовательность событий, связанных с этим продуктом. Кроме того, команда отключения маркера является недостаточно безопасной для защиты PII, поскольку длина пароля составляет только 32 бита, и функции команды отключения могут стать уязвимыми для атаки типа отказ в обслуживании, при которой злоумышленник отключает все маркеры вокруг себя.

II.2 Защита конфиденциальности с использованием физических технологий

II.2.1 Клетка Фарадея

Клетка Фарадея представляет собой технологию, которая не позволяет несанкционированному считывающему устройству RFID сканировать информацию на маркере, создавая помехи беспроводной передаче сигнала с этого устройства. Для этого используется контейнер, изготовленный из специальных материалов, блокирующих радиоизлучения. Для блокирования сигнала используется металлическая фольга. Несмотря на то что применение клетки может оказаться полезным в ряде областей, оно относительно ограничено, поскольку, если вынуть изделие из контейнера, функция защиты конфиденциальности утрачивается.

Рисунок II.1 – Футляр для паспорта/бумажник, защищенный клеткой Фарадея

II.2.2 Блокирующий маркер

Технология блокирующего маркера – технология, разработанная компанией RSA в 2003 году. Этот специальный маркер RFID предотвращает утечку информации, вызванную попыткой несанкционированного считывающего устройства нарушить связь между соседними маркерами путем генерации сигнала, содержащего бессмысленные данные. Например, маркер RFID содержит специальный бит, которому присваивается значение "общественный" или "частный". Для медицинского изделия, к которому прикреплен этот маркер, специальный бит до его продажи установлен в значение "общественный", а на прилавке после покупки значение меняется на "частный". Когда медицинское изделие с маркером, установленным в значение "общественный", вставляется в контейнер, в котором используется блокирующий маркер, информация на маркере изделия, устанавливаемая блокирующим маркером в значение "частное", не может быть считана другими лицами. Тем самым обеспечивается защита конфиденциальности покупателя.

II.2.3 Создание активных помех

Создание активных помех нарушает работу всех считывающих устройств RFID вблизи устройства. Для этого используется устройство, которое излучает мощные помехи. Таким образом, данная технология предотвращает утечку личной информации путем блокирования считывания информации, содержащейся на маркере RFID.

Отметим, что блокирующий маркер и создание активных помех – это простая технология, которая может легко использоваться для атак отказа обслуживания. Кроме того, они являются возможными решениями только на уровне пользователя, а не решениями, которые могут быть объединены в услуге RFID.

II.2.4 Усеченный маркер

Технология усеченного маркера была разработана компанией IBM, для того чтобы компенсировать недостатки команды деактивации, уменьшив дальность связи маркера путем срезания части соединительной линии антенны, расположенной внутри маркера. Эта технология способна свести к минимуму возможность нарушения конфиденциальности с использованием отслеживания местоположения из удаленного места, что достигается за счет существенного сокращения дальности передачи информации при одновременном сохранении функции хранения информации, выполняемой маркером.

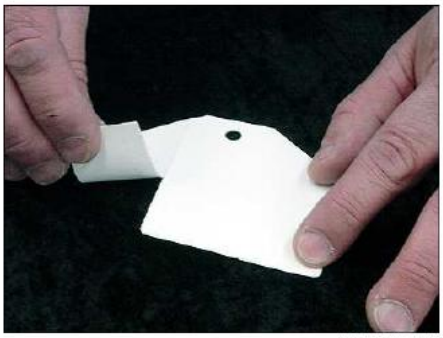

Рисунок II.2 – Усеченный маркер

II.2.5 RFID Zapper

RFID Zapper был представлен на Конгрессе связи, проводимом в Хаосе в 2005 году. Это электронное устройство, которое может окончательно деактивировать пассивные маркеры RFID. RFID Zapper был разработан для того, чтобы не повредить любому устройству, в отличие от других методов, таких как создание активных помех и усеченный маркер, здесь может быть подключен маркер RFID.

II.3 Защита конфиденциальности с использованием криптографических технологий

Следующие решения используют упрощенные протоколы шифрования для осуществления лучшей безопасности и защиты конфиденциальности на уровне маркера. Предлагаемые решения не являются достаточно зрелыми, для того чтобы эффективно использоваться в практическом применении, однако в данной области продолжаются многие научные исследования. Даже если они не применимы сегодня, предлагаемые решения дают хорошее представление о том, как законченное решение может

выглядеть в будущем. Отметим, что существует вероятность того, что данные протоколы потребуют изменений в настоящих стандартизированных протоколах радиосвязи [b-ISO/IEC 14443], [ISO/IEC 18000] или исследования в камках EPCGlobal).

II.3.1 Блокировка с использованием хеширования

При блокировке с использованием хеширования, которая является одним из характерных методов использования криптографической технологии, информация о маркере передается санкционированному считывающему устройству и внутреннему серверу только при условии, что подобрать обратную функцию для функции одностороннего хеширования будет трудно. Как подробно изображено на рисунке II.3, в ответ на запрос информации о маркере, направленный считывающим устройством, предоставляется только мета-идентификатор, который затем передается считывающему устройству после проверки правомерности получения им информации аутентификации от внутренней базы данных. Однако следует отметить, что при использовании данного метода возникает проблема, т. е. пользователя нельзя отследить, поскольку мета-идентификатор имеет статическое свойство и мог быть использован в качестве идентификатора маркера.

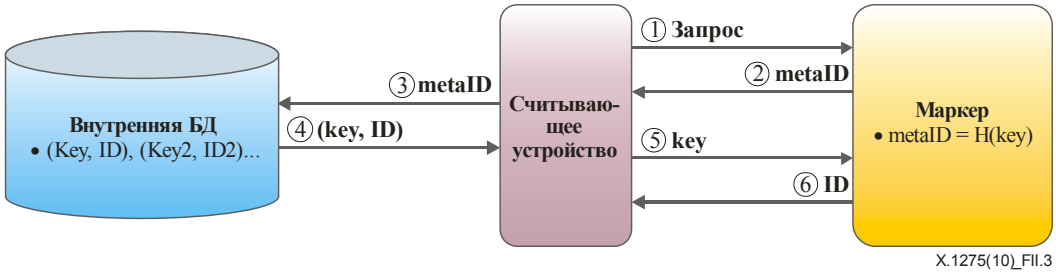

Рисунок II.3 – Блокировка с использованием хеширования

Метод блокировки с использованием рандомизированного хеширования является одним из методов, предназначенных для решения проблемы отслеживаемости пользователя при существующих методах блокировки с использованием хеширования. Как подробно изображено на рисунке II.4, данный метод может предотвратить отслеживание за счет использования генератора случайных чисел с хеш-функцией. Было предложено много других методов, основанных на хеш-функции, например цепочка хеширования, однако они были сочтены неприменимыми [b-Weis].

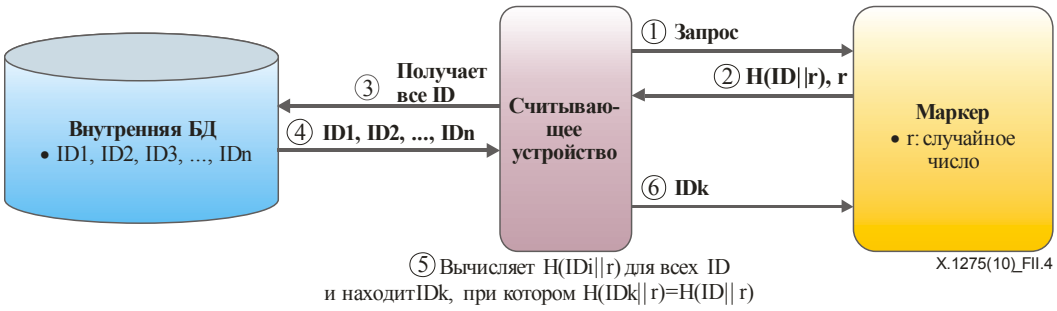

Рисунок II.4 – Рандомизированное хеширование

II.3.2 Повторное шифрование

Метод повторного шифрования позволяет собирать информацию на маркере только внутренней базе данных или считывающему устройству с открытым ключом внутренней базы данных, поскольку санкционированная внутренняя база данных или считывающее устройство через определенные промежутки времени шифруют идентификацию маркера с открытым ключом и сохраняют созданную информацию на маркере. Протокол повторного шифрования основан на ElGamal и состоит из двух шагов. Сначала внутренняя база данных конца создает C, используя открытый ключ и случайное число, а затем сохраняет C на маркере. Второй шаг подробно изображен на рисунке II.5.

Этот метод может применяться к записям, обладающим высокой ценностью. Если используется этот метод, то периодическое шифрование предотвращает отслеживание информации на маркере RFID. Тем не менее существует угроза утечки информации путем несанкционированного подключения во время передачи открытого ключа, поскольку используется метод шифрования открытым ключом. Кроме того, методы, основанные на шифровании с использованием открытого ключа, например повторное шифрование, не могут применяться в дешевых пассивных маркерах, используя имеющиеся в настоящее время технологии.

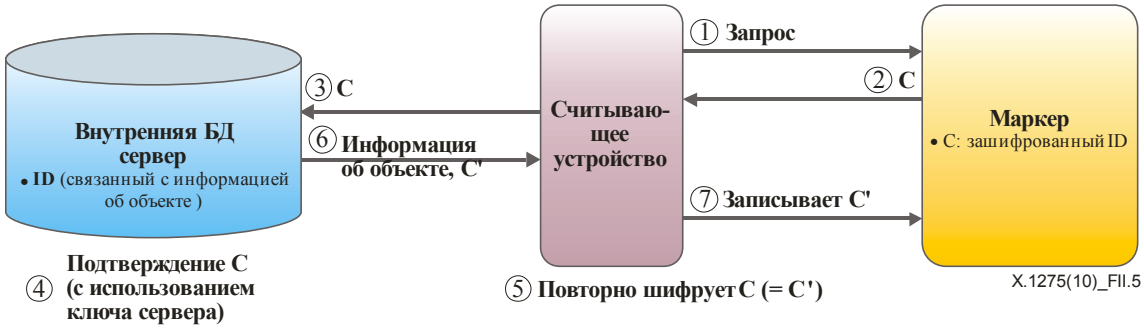

Рисунок II.5 – Повторное шифрование

Библиография

[b-Council of Europe] Council of Europe, "*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*", 1981. http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm.

[b-CRYPTREC] Telecommunications Advancement Organization of Japan, "*CRYPTREC Report 2002*", March 2003, Information-technology Promotion Agency, Japan.

[b-DSTI/ICCP] "*RFID, OECD Policy Guidance, A Focus on Information Security and Privacy, Applications, Impacts and Country Initiatives*", OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, Korea, 17-18 June 2008.

[b-EC1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 1995. http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[b-EC2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

[b-EPIC] Electronic Privacy Information Center, "*Guidelines on Commercial Use of RFID Technology*", July 2004.

[b-E-Zpass] http://www.ezpass.com/static/info/howit.shtml.

[b-ICAO] ICAO, Doc 9303, *Machine Readable Travel Documents*, Part 1, Volume 2, 6th edition, 2006.

[b-IPC] Information and Privacy Commissioner/Ontario, "*Privacy Guidelines for RFID information Systems (RFID Privacy Guidelines)* ", June 2006.

[b-Isamu Y] Isamu, Y., Shinichi, S., Akira, I. and Satoshi, I., "*Secure Active RFID Tag System"*, 7th International Conference on Ubiquitous Computing, September 2005.

[b-ISO 22307] ISO 22307:2008, "*Financial services – Privacy impact assessment*", August 2008.

[b-ISO/IEC 14443] ISO/IEC 14443:2008, Идентификационные карты – Бесконтактные карты с интегральной схемой – Карты малой дальности действия.

[b-Japan] MIC (Ministry of Internal Affairs and Communications), METI (Ministry of Economy, Trade and Industry) Government of Japan, "*Guidelines for Privacy Protection with Regard to RFID Tags*", July 2004.

[b-Juels] Juels, A., Rivest, R.L., and Szydlo, M., "*The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*", ACM Conference on Computer and Communications Security, 2003.

[b-Junichiro] Junichiro Saito, Jae-Cheol Ryou, and Kouichi Sakurai, "*Enhancing privacy of Universal Re-encryption scheme for RFID tags*", Embedded and Ubiquitous Computing 2004.

[b-Korea] MIC (Ministry of Information and Communication) of Korea, "*RFID Privacy Protection Guideline*", July 2005.

[b-NIST] NIST SP 800-98, "*Guidance for Securing Radio Frequency Identification (RFID) Systems*", September 2007.

[b-OECD] OECD, "*Guideline on the Protection of Privacy and Transborder Flows of Personal Data*", 1980.

[b-Peris-Lopez] Pedro Peris-Lopez *et al*, "*M^2 AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags*", 3rd International Conference on Ubiquitous Intelligence and Computing, September 2006.

[b-PIA Canada] Treasury Board of Canada Secretariat, "*Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*", 2002. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld2-eng.asp.

[b-PIA Korea] MIC (Ministry of Information and Communication) of Korea, "*Privacy Impact Assessment Guideline for Private Sector*", December 2005.

[b-Simon L1] Simson, L., Garfinkel, Ari Juels, and Ravi Pappu, "*RFID Privacy: An Overview of Problems and Proposed Solutions*", IEEE Security and Privacy, 2005.

[b-Simon L2] Simson, L., Garfinkel and Beth Rosenberg, "*RFID: Applications, Security, and Privacy*", Addison-Wesley Professional, July 2005.

[b-UNHCR] UN General Assembly, "*Guidelines for the Regulation of Computerized Personal Data Files*", 1990. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08, PDF/G9010708-pdf.

[b-Weis] Weis S., *et al.*, "*Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems*", Security and Pervasive Computing 2003.

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, 2011 г.