Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2740

(01/2011)

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

Сети последующих поколений – Безопасность

Требования к безопасности мобильных дистанционных финансовых транзакций в сетях последующих поколений

Рекомендация МСЭ-Т Y.2740

ITU-T

ITU Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие положения	Y.100–Y.199
Услуги, приложения и промежуточные программные средства	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и присваивание имен	Y.500–Y.599
Эксплуатация, управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Рабочие характеристики	Y.800–Y.899
АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ	
Общие положения	Y.1000–Y.1099
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, возможности сетей и административное управление ресурсами	Y.1200–Y.1299
Транспортирование	Y.1300–Y.1399
Взаимодействие	Y.1400–Y.1499
Качество обслуживания и сетевые показатели качества	Y.1500–Y.1599
Сигнализация	Y.1600–Y.1699
Эксплуатация, управление и техническое обслуживание	Y.1700–Y.1799
Начисление платы	Y.1800–Y.1899
IPTV по СПП	Y.1900–Y.1999
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	
Структура и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты обслуживания: возможности услуг и архитектура услуг	Y.2200–Y.2249
Аспекты обслуживания: взаимодействие услуг и СПП	Y.2250–Y.2299
Нумерация, присваивание имен и адресация	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
Будущие сети	Y.2600–Y.2699
Безопасность	**Y.2700–Y.2799**
Обобщенная мобильность	Y.2800–Y.2899
Открытая среда операторского класса	Y.2900–Y.2999
Будущие сети	Y.3000–Y.3099

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

Рекомендация МСЭ-Т Y.2740

Требования к безопасности мобильных дистанционных финансовых транзакций в сетях последующих поколений

Резюме

В течение последних нескольких лет было создано большое число разнообразных сетей дистанционных платежей с использованием сетей подвижной связи. Несмотря на реализацию разных подходов, они зачастую не обеспечивают безопасности. В то же время сети связи, в том числе сети подвижной связи, претерпевают существенные изменения в связи с переходом на сети последующих поколений (СПП).

В Рекомендации МСЭ-Т Y.2740 рассматриваются подходы к разработке системы безопасности для мобильной коммерции и мобильного банкинга в сетях последующих поколений (СПП). Описываются требования к безопасности систем мобильной коммерции и мобильного банкинга, основанные на четырех установленных уровнях безопасности. Указаны возможные риски, существующие в системах мобильной коммерции и мобильного банкинга, и определяются средства снижения рисков.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т Y.2740	28.01.2011 г.	13-я

Ключевые слова

Мобильный банкинг, мобильная коммерция, мобильные платежи, дистанционные платежи, безопасность.

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

© ITU 2011

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

СОДЕРЖАНИЕ

		Стр.
1	Сфера применения	1
2	Справочные документы	1
3	Определения	1
	3.1 Термины, определенные в других документах	1
	3.2 Термины, определенные в настоящей Рекомендации	2
4	Сокращения и акронимы	2
5	Условные обозначения	2
6	Соображения, касающиеся безопасности систем мобильного банкинга и мобильной коммерции в сетях последующих поколений	3
	6.1 Основные риски, связанные с мобильными дистанционными финансовыми транзакциями	3
	6.2 Цели безопасности	3
	6.3 Уровни безопасности и средства их поддержки	3
Библиография		8

Рекомендация МСЭ-Т Y.2740

Требования к безопасности мобильных дистанционных финансовых транзакций в сетях последующих поколений

1 Сфера применения

В настоящей Рекомендации описываются риски безопасности, которые связаны с дистанционными мобильными финансовыми транзакциями, поддерживаемыми прикладными услугами сетей последующих поколений (СПП), а также меры, направленные на снижение риска и противодействие ему, которые базируются на четырех уровнях безопасности. Наряду с этим в настоящей Рекомендации определяются минимальные, касаются дистанционных мобильных финансовых транзакций, требования по защите неприкосновенности частной жизни в отношении персональных данных частных лиц.

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 статуса Рекомендации.

[ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[ITU-T X.805] Рекомендация МСЭ-Т X.805 (2003 г.), *Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами*.

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

[ITU-T Y.2741] Recommendation ITU-T Y.2741 (2011), *Architecture of secure mobile financial transactions in the next generation networks*.

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) [ITU-T X.800]: Предотвращение несанкционированного использования какого-либо ресурса, в том числе предотвращение использования ресурса в режиме несанкционированных действий.

3.1.2 приложение (application) [ITU-T Y.2741]: Специальное приложение мобильного банкинга или мобильной коммерции, закачанное на мобильное устройство клиента (пользователя).

3.1.3 аутентификация (authentification) [ITU-T X.800]: См. "аутентификация источника данных" и "аутентификация однорангового объекта".

ПРИМЕЧАНИЕ. – В настоящей Рекомендации термин "аутентификация" не используется в сочетании с целостностью данных, вместо него используется термин "целостность данных".

3.1.4 готовность (availability) [ITU-T X.800]: Свойство, обеспечивающее доступность и годность к использованию по запросу авторизованного объекта.

3.1.5 клиент (client) [ITU-T Y.2741]: Физическое или юридическое лицо, с которым заключен договор на использование услуг связи и услуг системы мобильной коммерции.

3.1.6 конфиденциальность (confidentiality) [ITU-T X.800]: Свойство, не допускающее раскрытия информации неавторизованным частным лицам, объектам или процессам.

3.1.7 целостность данных (data integrity) [ITU-T X.800]: Свойство, не допускающее изменения или уничтожения данных несанкционированным образом.

3.1.8 аутентификация источника данных (data origin authentication) [ITU-T X.800]: Подтверждение того, что источник принятых данных соответствует объявленному.

3.1.9 система мобильных платежей (mobile payment system) [ITU-T Y.2741]: Система мобильного банкинга и/или мобильной коммерции.

3.1.10 сети последующих поколений (next generation network) (NGN) [b-ITU-T Y.2001]: Сети с коммутацией пакетов, которые могут предоставлять услуги электросвязи и использовать несколько широкополосных технологий транспортирования с поддержкой функции QoS и в которых связанные с услугами функции не зависят от лежащих в основе технологий транспортирования. Эти сети обеспечивают пользователям беспрепятственный доступ к сетям и конкурирующим поставщикам услуг и к услугам по выбору пользователей. Они поддерживают универсальную мобильность, которая обеспечивает постоянное и повсеместное предоставление услуг пользователям.

3.1.11 неприкосновенность частной жизни (privacy) [ITU-T X.800]: Право частных лиц контролировать или оказывать влияние на то, какая касающаяся их информация может быть собрана и храниться, кто эту информацию может раскрывать и кому она может быть раскрыта.

ПРИМЕЧАНИЕ. – В силу того что этот термин относится к правам частных лиц, он не может быть очень точным, и следует избегать его использования, за исключением мотивирования требования обеспечения безопасности.

3.1.12 непризнание участия (repudiation) [ITU-T X.800]: Отказ одного из объектов, участвующих в соединении, от того, что он участвовал во всем процессе или в части этого процесса.

3.1.13 параметр безопасности (security dimension) [ITU-T X.805]: Совокупность мер безопасности, разработанных для обеспечения определенного аспекта безопасности сети.

3.1.14 уровень безопасности (security layer) [ITU-T X.805]: Иерархия сетевого оборудования и группировки сетевых средств.

3.1.15 плоскости безопасности (security planes) [ITU-T X.805]: Определенный тип сетевой деятельности, защищенный параметрами безопасности.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации используется следующий термин:

3.2.1 уровень безопасности (security level): Спецификация безопасности системы, в которой определяется эффективность защиты от рисков.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

GSM	Global System for Mobile Communications		Глобальная система подвижной связи
MPS	Mobile Payment System		Система мобильных платежей
MSISDN	Mobile Station International ISDN Number		Международный номер ЦСИС подвижной станции
NGN	Next Generation Network	СПП	Сети последующих поколений
PA-DSS	Payment Application Data Security Standard		Стандарт безопасности данных платежных приложений
PCI DSS	Payment Card Industry Data Security Standard		Стандарт безопасности данных индустрии платежных карт

5 Условные обозначения

Не применяются.

6 Соображения, касающиеся безопасности систем мобильного банкинга и мобильной коммерции в сетях последующих поколений

Безопасность систем мобильных платежей (MPS) в сетях последующих поколений (СПП) обеспечивается на основе архитектуры MPS и ролей участников MPS, определенных в [ITU-T Y.2741], *Architecture of secure mobile financial transactions in next generation networks*, а также на основе анализа рисков участников MPS, описанных ниже.

6.1 Основные риски, связанные с мобильными дистанционными финансовыми транзакциями

В данном пункте не рассматриваются факторы появления новых глобальных и индустриальных рисков участников при внедрении систем мобильных платежей – системных, стратегических, относящихся к странам и суверенитету, рыночных, процентных, рисков ликвидности, правовых, репутационных и т. п. В нем рассматриваются лишь информационные риски, которые могут непосредственно возникать при использовании дистанционных мобильных платежей и которые требуют решения вопросов безопасности в целях сведения их к минимуму:

- риск потери конфиденциальности, подразумевающий несанкционированный доступ к конфиденциальной информации;
- риск нарушения целостности данных, при котором происходит искажение информации в процессе передачи или обработки;
- риск подделки электронных документов (риск для аутентичности), когда электронные документы формируются неавторизованными участниками;
- риск непризнания участия, включающий отказ от авторства электронного документа;
- риск уничтожения информации умышленно или по халатности;
- транзакционный риск, подразумевающий невозможность завершения транзакции вследствие плохого качества передачи.

6.2 Цели безопасности

Для обеспечения безопасности мобильного платежа и снижения рисков участников решение должно обеспечивать достижение следующих целей:

- уменьшить возможность перехвата персональной или финансовой информации во время транзакции;
- уменьшить возможность извлечения персональной или финансовой информации из баз данных;
- уменьшить возможность подмены или искажения персональной или финансовой информации во время транзакции;
- уменьшить возможность использования решения неавторизованными лицами и лицами, пытающимися использовать маскировку, путем реализации однозначной аутентификации;
- уменьшить возможность использовать "украденную" информацию в решении;
- обеспечить основания, для того чтобы инициатору или участнику транзакции было невозможно отказаться от своих действий после их совершения;
- обеспечить соблюдение законных прав и обязанностей всех участников взаимодействия;
- обеспечить завершение транзакции.

6.3 Уровни безопасности и средства их поддержки

В настоящей Рекомендации описываются четыре уровня безопасности MPS на основе анализа рисков участников MPS.

Уровень безопасности системы определяется совокупностью реализации параметров безопасности (см. таблицу 1). Следовательно, безопасность четвертого (высшего) уровня должна характеризоваться наиболее стойкой реализацией параметров безопасности. Вместе с тем требования к ряду параметров безопасности являются едиными для всех уровней безопасности.

Стороны, использующие MPS, должны быть осведомлены об уровне безопасности системы и рисках системы.

Приемлемый уровень безопасности в отношении определенного риска любого компонента системы определяется стороной, принимающей данный риск.

Стороны могут дополнительно снизить риски, связанные с использованием MPS, с помощью эксплуатационных мер, которые могут включать ограничение частоты или денежной ценности отдельных транзакций, готовность услуги для пользователей с высоким уровнем лояльности и т. д.

Клиент идентифицирует себя в системе с помощью сетевого открытого идентификатора СПП (например, MSISDN для сетей GSM).

6.3.1 Реализация параметров безопасности для всех уровней безопасности

Осуществление безопасности системы возложено на всех участников системы и достигается с помощью физических и административных средств обеспечения безопасности при передаче, обработке и хранении данных. Участники системы должны обеспечивать реализацию отраслевых стандартов информационной безопасности (например, [b-PCI DSS], [b-PA-DSS] и т. д.).

Ниже приводится перечень восьми параметров безопасности [ITU-T X.805], которые определяют уровни безопасности MPS. Требуется обязательная реализация всеми участниками системы параметров безопасности применительно к информации, участвующей в обмене данными.

1) Управление доступом: доступ к каждому компоненту MPS должен предоставляться только в соответствии с уровнем доступа персонала или конечных пользователей системы. Это требование действует на всех уровнях безопасности.

2) Аутентификация: должна обеспечиваться аутентичность заявленной идентичности участвующих объектов. Данное требование является одним из основных факторов снижения риска отказа от авторства. В связи с широкими организационно-техническими возможностями реализации, на каждом уровне безопасности определяются минимальные требования к механизму аутентификации.

   Существуют следующие три фактора аутентификации клиента (пользователя):

   – клиент использует какую-либо информацию, которая больше никому не может быть известна, например пароль для доступа ("нечто известное");

   – клиент обладает чем-либо, что имеется только у него, и однозначным образом выполняет определенные действия, например генерирует электронную подпись или код аутентификации сообщения ("нечто имеющееся");

   – клиент использует биометрические данные ("нечто личное").

3) Предотвращение отказа от участия: обеспечивает средство, позволяющее не допустить отказа частного лица или объекта от совершения какого-либо конкретного действия (например, отправления, пересылки или приема сообщений). С этой целью все действия персонала и конечных пользователей системы должны подвергаться обязательной регистрации. Журналы регистрации событий должны быть защищены от изменений и содержать все действия всех пользователей. Соблюдение этих требований достигается с помощью средств, которые юридически закреплены или зарезервированы в двусторонних договорах, а также с помощью принятых механизмов аутентификации. Это требование действует на всех уровнях безопасности.

4) Конфиденциальность данных: используемые в системе данные защищены от несанкционированного раскрытия и изменения. Требования к конфиденциальности определяются критичностью данных системы. На каждом уровне безопасности определяются конкретные средства обеспечения конфиденциальности и накладываются ограничения на уровень критичности данных системы.

5) Безопасность связи: гарантированная доставка последовательности сообщений в обоих направлениях (адресату и от адресата), а также завершение транзакции (с использованием протоколов, обеспечивающих завершение транзакции) и защита информации от несанкционированного раскрытия в момент передачи по каналам связи. Это требование действует на всех уровнях безопасности.

6) Целостность данных: правильность, точность и целостность данных обеспечивается с помощью защиты от несанкционированного изменения, удаления, создания и тиражирования, а также указания на эти несанкционированные действия. Логическое завершение транзакции гарантируется при выполнении определенных условий, которые реализуются на уровне приложения. На каждом уровне безопасности определяются конкретные механизмы обеспечения целостности. Обеспечение целостности может достигаться за счет конфиденциальности данных и управления доступом.

7) Готовность: обеспечение сохранения санкционированного доступа к данным и услугам MPS. Это требование действует на всех уровнях безопасности и должно выполняться поставщиком услуг по принципу "лучшее из возможного".

8) Неприкосновенность частной жизни: обеспечивает безопасность информации, которая участвует в обмене данными и хранится у участников системы. В решении должно использоваться минимальное количество данных, необходимых для работы системы. Участники системы должны снижать вероятность несанкционированных получения и передачи данных. Система должна обеспечивать соблюдение стандартов финансового сектора.

На всех уровнях безопасности равным образом реализуются следующие параметры безопасности:

– управление доступом;
– предотвращение отказа от участия;
– безопасность связи;
– готовность.

Следующие параметры безопасности по-разному реализуются на разных уровнях безопасности:

– аутентификация;
– конфиденциальность данных;
– целостность данных;
– неприкосновенность частной жизни.

6.3.2 1-й уровень безопасности

MPS может полагаться на аутентификацию клиента, обеспечиваемую оператором СПП.

Конфиденциальность и целостность данных обеспечивается за счет среды передачи данных (безопасности связи), а при их хранении и обработке – с помощью механизма хранения данных, а также средств управления доступом в систему.

Неприкосновенность частной жизни обеспечивается за счет отсутствия в передаваемых сообщениях данных, требующих защиты, а также с помощью реализации необходимых механизмов хранения данных и средств управления доступом в систему. Компоненты системы не должны иметь скрытых возможностей по несанкционированным получению и передаче данных.

6.3.3 2-й уровень безопасности

Аутентификация при использовании услуг системы может осуществляться с помощью только одного фактора аутентификации и, следовательно, может быть реализована без применения криптографических протоколов.

Для аутентификации используется одноразовый пароль, который генерируется с помощью различных жетонов (однофакторное устройство генерирования одноразовых паролей, однофакторное криптографическое устройство и т. д.).

Конфиденциальность и целостность данных, а также неприкосновенность частной жизни обеспечиваются так же, как и на 1-м уровне.

6.3.4 3-й уровень безопасности

Для доступа к услугам системы должна использоваться многофакторная аутентификация клиента.

Для аутентификации клиента система должна использовать более одного фактора аутентификации.

Конфиденциальность и целостность данных, а также неприкосновенность частной жизни при передаче сообщения должна обеспечиваться с помощью дополнительного шифрования сообщения, а также протоколов передачи данных, которые обеспечивают безопасность данных, передаваемых участниками взаимоотношений (включая верификацию целостности данных). При хранении и обработке данных их конфиденциальность и целостность, а также неприкосновенность частной жизни обеспечиваются с помощью дополнительных механизмов шифрования и маскирования, наряду с четко определенным распределением доступа в соответствии с привилегиями и правами допуска.

Для выполнения требований к безопасности на данном уровне система должна использовать специальные прикладные программы, закачанные на мобильные устройства клиента. Эти прикладные программы должны реализовывать двухфакторную аутентификацию и обеспечивать шифрование и дешифрование передаваемых данных.

При каждом выполнении аутентификации должен требоваться ввод пароля или других данных активации, для того чтобы активировать ключ аутентификации, а незашифрованная копия ключа аутентификации должна удаляться после каждой аутентификации (многофакторный программный криптографический жетон).

Все участники взаимоотношений MPS должны использовать средства безопасности, которые обеспечивают стойкость системы к взлому. В случае решений 3-го уровня безопасность данных, передаваемых по каналам связи, должна обеспечиваться с помощью стойкой криптографии. Стойкость криптографических методов зависит от используемого криптографического ключа. Эффективный размер ключа должен соответствовать рекомендациям по выбору минимального размера ключа, при котором гарантируется его относительная стойкость.

6.3.5 4-й уровень безопасности

Данный уровень безопасности системы является самым высоким. Для выполнения требований к безопасности на данном уровне система должна использовать аппаратные модули безопасности, установленные в мобильных устройствах клиентов. Эти аппаратные модули безопасности должны реализовывать двухфакторную аутентификацию и обеспечивать шифрование и дешифрование передаваемых данных. При каждом выполнении аутентификации должен требоваться ввод пароля или других данных активации, для того чтобы активировать ключ аутентификации, а незашифрованная копия ключа аутентификации должна удаляться после каждой аутентификации (многофакторный аппаратный криптографический жетон). Для шифрования сообщений применяются алгоритмы как симметричного, так и несимметричного шифрования.

Реализация других параметров безопасности должна полностью соответствовать 3-му уровню.

Таблица 1 – Корреляция уровней безопасности и реализации параметров безопасности

<table>
<tr><th rowspan="2">Параметр безопасности</th><th colspan="4">Уровень безопасности</th></tr>
<tr><th>1-й уровень</th><th>2-й уровень</th><th>3-й уровень</th><th>4-й уровень</th></tr>
<tr><td>Управление доступом</td><td colspan="4">Доступ к каждому компоненту системы должен предоставляться только авторизованному персоналу системы. Активацию специальных прикладных программ, закачанных на мобильные терминалы, следует разрешать только авторизованным клиентам</td></tr>
<tr><td>Аутентификация</td><td>Аутентификация в системе обеспечивается за счет среды передачи данных СПП</td><td>Использование однофакторной аутентификации в услугах системы</td><td>Использование многофакторной аутентификации в услугах системы</td><td>Личный контракт на услуги, в котором используются персональные данные с обязательной идентификацией.
Использование многофакторной аутентификации в услугах системы.
Обязательное использование аппаратного криптографического модуля</td></tr>
<tr><td>Предотвращение отказа от участия</td><td colspan="4">Невозможность для инициатора транзакции или участника отказаться от своих действий после их завершения обеспечивается прямыми или косвенными юридическими условиями контрактов, которые юридически закреплены или зарезервированы в двусторонних договорах, а также с помощью принятых механизмов аутентификации. Все действия персонала и конечных пользователей системы должны регистрироваться. Журналы регистрации событий должны быть защищенными от изменений и содержать все действия всех пользователей</td></tr>
<tr><td>Конфиденциальность данных
Целостность данных</td><td colspan="2">Конфиденциальность данных в процессе их передачи обеспечивается за счет среды передачи данных (безопасности связи), а при их хранении и обработке – с помощью механизма хранения данных, а также средств управления доступом системы</td><td rowspan="2">Конфиденциальность данных в процессе их передачи обеспечивается с помощью дополнительного шифрования сообщения, а также протоколов передачи данных, которые обеспечивают безопасность данных, передаваемых участниками взаимоотношений (включая верификацию целостности данных).
В процессе хранения и обработки данных их конфиденциальность, целостность, а также неприкосновенность частной жизни обеспечиваются с помощью дополнительных механизмов шифрования и маскирования, наряду с четко определенным распределением доступа в соответствии с привилегиями и правами допуска</td><td rowspan="2">Реализация требований 3-го уровня с обязательным использованием аппаратных криптографических средств и средств обеспечения безопасности данных на стороне клиента (аппаратного криптографического модуля)</td></tr>
<tr><td>Неприкосновенность частной жизни</td><td colspan="2">Неприкосновенность частной жизни обеспечивается за счет отсутствия в передаваемых сообщениях данных, требующих защиты, а также с помощью реализации необходимых механизмов хранения данных и средств управления доступом системы.
Компоненты системы не должны иметь скрытых возможностей по несанкционированным получению и передаче данных</td></tr>
<tr><td>Безопасность связи</td><td colspan="4">Гарантируется доставка сообщения адресату, а также защита информации от несанкционированного раскрытия в момент передачи по каналам связи. Это требование обеспечивается операторами СПП</td></tr>
<tr><td>Готовность</td><td colspan="4">Обеспечивается отсутствие отказа в санкционированном доступе к данным и услугам системы. Готовность обеспечивается операторами СПП, а также поставщиками услуг MPS</td></tr>
</table>

Библиография

[b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

[b-PA-DSS] Payment Card Industry (PCI), *Payment Application Data Security Standard. Requirements and Security Assessment Procedures*, Version 2.0, October 2010.

[b-PCI DSS] Payment Card Industry (PCI), *Data Security Standard. Requirements and Security Assessment Procedures*, Version 2.0, October 2010.

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.