Центральный банк Российской Федерации

П Р С

Платежные и расчетные системы

Международный опыт

Выпуск 21

Стандарты наблюдения за европейскими розничными платежными системами

Наблюдение за платежными схемами, функционирующими с использованием карт. Стандарты

Наблюдение за системами прямого дебета. Стандарты

Наблюдение за системами кредитовых переводов. Стандарты

2010

107016, Москва, ул. Неглинная, 12

Материалы подготовлены Департаментом регулирования расчетов Центрального банка Российской Федерации
E-mail: prs@cbr.ru, тел. 771-45-64, факс 771-97-11

Текст данного сборника размещен на сайте Центрального банка Российской Федерации в сети Интернет:
http://www.cbr.ru

Издатель: ЗАО "АЭИ "ПРАЙМ-ТАСС"
125009, Москва, Тверской б-р, 2
Тел. 974-76-64, факс 692-36-90, www.prime-tass.ru, e-mail: sales01@prime-tass.ru

Отпечатано в типографии "Полиграфическая компания "СТАМПА ВИВА"
109052, г. Москва, ул. Подъемная, 14, стр. 4А

Содержание

СТАНДАРТЫ НАБЛЮДЕНИЯ ЗА ЕВРОПЕЙСКИМИ РОЗНИЧНЫМИ ПЛАТЕЖНЫМИ СИСТЕМАМИ

Европейский центральный банк

Июнь 2003 г.

Содержание

1. Введение*

Наблюдение за платежными системами является неотъемлемой функцией центральных банков и имеет своей целью обеспечить бесперебойное функционирование платежных систем и финансовую стабильность. Функция наблюдения Евросистемы[1] определена в "Учредительном договоре Европейского сообщества" (далее именуемом "Договор") и "Уставе Европейской системы центральных банков (ЕСЦБ) и Европейского центрального банка (ЕЦБ)" (далее именуемом "Устав"). Статья 105 (2) Договора и Статья 3 Устава гласят: *"основные задачи ЕСЦБ... обеспечить бесперебойное функционирование платежных систем".*

Задача Евросистемы содействовать бесперебойному функционированию платежных систем заключается в обеспечении безопасности и эффективности платежных систем, а также защищенности платежных инструментов. Роль Евросистемы в области наблюдения за платежными системами была описана в публичном заявлении 2000 года[2]. В нем были утверждены минимальные стандарты политики наблюдения за платежными системами, которым провайдеры платежных услуг должны отвечать. Примерами таких стандартов могут служить "Доклад об электронных деньгах" 1998 года[3] и стандарты Группы десяти "Ключевые принципы для системно значимых платежных систем"[4] ("Ключевые принципы"), которые были утверждены Советом управляющих ЕЦБ в январе 2001 года.

Настоящий документ конкретизирует стандарты наблюдения, применяемые к розничным платежным системам еврозоны, включая национальные и общеевропейские системы. В нем дается методология, которой пользуется Евросистема для определения различных категорий розничных платежных систем, и разъясняется, какие стандарты применяются к каждой категории. В частности, определены подходы к новым стандартам для розничных платежных систем, играющих важную роль в функционировании экономики. Дополнительно Евросистема пересмотрела то, каким образом в государствах — участниках ЕС осуществляется регистрация розничных платежных систем в соответствии со статьей 10 "Директивы о завершении расчетов" (ДЗР).

2. Классификация розничных платежных систем еврозоны

ЕЦБ и национальные центральные банки во исполнение своих функций по наблюдению сформировали методологию классификации розничных платежных систем и применения соответствующих стандартов в еврозоне. В зависимости от возможной степени ущерба финансовым рынкам и/или экономике в целом при возникновении сбоев в функционировании розничных платежных систем еврозоны последние должны будут соответствовать сбалансированному набору стандартов наблюдения. Розничная платежная система, сбой в которой может угрожать стабильности финансовых рынков, именуется в дальнейшем системно значимой розничной платежной системой (СиРПС), согласно Евросистеме должна отвечать всему набору "Ключевых принципов". Розничная платежная система, сбой в которой не влечет за собой системных последствий, но тем не менее может оказать серьезное воздействие (с учетом того обстоятельства, что рассматриваемая система важна для реальной экономики), именуется в дальнейшем социально значимой розничной платежной системой (СоРПС). Она должна отвечать требованиям подраздела "Ключевых принципов", далее именуемого "Розничные стандарты". Розничная платежная система, не принадлежащая ни к одной из двух вышеописанных категорий, должна отвечать соответствующим стандартам наблюдения для подобных систем (если таковые имеются)[5].

---

* Данный материал является неофициальным переводом публикации ЕЦБ "Oversight standards for euro retail payment systems" ("Стандарты наблюдения за европейскими розничными платежными системами"). Электронная версия данной публикации на английском языке размещена на веб-сайте ЕЦБ *(www.ecb.int/pub/pdf/other/retailpsoversightstandardsen.pdf).*

[1] Евросистема охватывает ЕЦБ и национальные центральные банки государств — участников Евросоюза, которые используют евро.

[2] ЕЦБ, "Роль Евросистемы в области наблюдения за платежными системами", 2000 год.

[3] ЕЦБ, "Доклад об электронных деньгах", 1998 год.

[4] Банк международных расчетов, "Ключевые принципы для системно значимых платежных систем" (так называемые "Ключевые принципы"), 2001 год.

[5] Как разъясняется в заявлении ЕЦБ "Роль Евросистемы в области наблюдения за платежными системами" (выходные данные которого указаны выше), национальные банки могут дополнять описываемую общую политику наблюдения специфическими мерами, непосредственно рассчитанными на подобные розничные системы.

2.1. Системно значимые розничные платежные системы

“Ключевые принципы” содействуют развитию безопасных и эффективных платежных систем и устанавливают стандарты, применимые ко всем СиРПС в международном масштабе. В соответствии с “Ключевыми принципами” платежная система рассматривается как системно значимая, если она способна спровоцировать сбой или распространить негативные воздействия на всю национальную или даже международную финансовую систему. Главными критериями являются объем и характер платежей, которые через нее осуществляются. Платежная система, вероятнее всего, будет обладать системной значимостью, если она отвечает хотя бы одному из следующих условий:

1) она является единственной национальной платежной системой или доминирует по совокупному объему платежей;

2) через нее главным образом осуществляются крупные платежи; или

3) она используется для расчетов по операциям финансового рынка или для расчетов других платежных систем.

Каждая СиРПС должна отвечать всем десяти “Ключевым принципам”. В то время как все платежные системы для крупных сумм в еврозоне имеют системную значимость, некоторые розничные платежные системы могут также быть системно значимыми и, следовательно, должны полностью выполнять все “Ключевые принципы”. Центральные банки Евросистемы периодически анализируют розничные платежные системы еврозоны и могут квалифицировать некоторые розничные платежные системы как СиРПС.

При оценке системной значимости розничной платежной системы ЕЦБ и национальные центральные банки должны принимать во внимание долю ее участия в операциях на соответствующем рынке розничных платежей, финансовые риски, а также вероятность риска “эффекта домино”. Им следует руководствоваться следующими показателями:

- *Доля участия в рыночных операциях [проникновение на рынок].* В странах, где нет альтернативной розничной платежной системы, в случае ее банкротства будет отсутствовать альтернативный канал, через который население сможет осуществлять розничные платежи. Объемы платежей, проходящих через подобную систему, обычно слишком велики, чтобы быть обработанными через систему валовых расчетов в режиме реального времени (ВРРВ). Схожая картина складывается и тогда, когда существует несколько розничных платежных систем, одна из которых обрабатывает основную часть платежей. Кроме того, технические стандарты рассматриваемых платежных систем могут отличаться от стандартов систем ВРРВ и иных розничных систем, что делает технически невозможным осуществление розничных платежей, даже если их объемы могут быть обработаны системой. Таким образом, банкротство единственной или доминирующей [обрабатывающей основную часть платежей] системы угрожает подорвать доверие большинства населения данной страны к платежной системе и валюте. Следовательно, если в стране отсутствует альтернативная платежная система или соглашение, которое позволяет осуществлять розничные платежи, или если система занимает значительную долю рынка, то данная ситуация заслуживает пристального внимания. Значительная доля соответствующего рынка подразумевает охват более 75% его платежей, осуществляемых через межбанковские розничные платежные системы и иные платежные соглашения.

- *Совокупные финансовые риски.* Важным фактором при оценке того, системно значима ли розничная платежная система, является объем обрабатываемых платежей. Вследствие этого в “Ключевых принципах” придается большое значение объему платежей, поскольку существует прямая зависимость между обрабатываемыми суммами и степенью кредитного риска и риска ликвидности: чем выше суммы, обрабатываемые системой, тем выше системное воздействие. Даже если отдельные розничные платежные системы не лидируют по совокупной стоимости платежей, они могут обрабатывать платежи совокупной стоимости, имеющей большое значение для финансовой системы. Для оценки системного воздействия будет полезно сопоставить суммы, обрабатываемые как розничной платежной системой, так и соответствующей системой ВРРВ. Все системы ВРРВ в еврозоне являются системно значимыми. Чрезвычайно высокие суммы платежей тоже служат показателем системной значимости. Следовательно, особое внимание должно быть уделено розничным платежным системам, обрабатывающим более 10% совокупных объемов соответствующей системы ВРРВ или обрабатывающим платежи, средний ежедневный объем которых превышает 10 миллиардов евро.

- *Риск “эффекта домино”.* Неспособность одного участника розничной платежной системы отвечать по своим обязательствам может иметь серьезные последствия для остальных, продолжающих отвечать по своим обязательствам, поскольку проблемы отдельных участников могут оказать негативное воздействие и на них. При наихудшем сценарии развития ситуации подобные проблемы могут распространиться на всех участников системы. Очевидно, что риску “эффекта домино” наиболее подвержены системы нетто-расчетов, однако и в системе валовых расчетов неспособность одного из участников выполнять свои обязательства

может послужить причиной сокращения ликвидности в системе. Элементами, которые могут способствовать возникновению "эффекта домино", являются степень концентрации, или эффект неттинга в системе, или же размер дебетовой нетто-позиции участников.

Если участник с самыми крупными обязательствами в платежной системе неспособен их выполнять, а обрабатываемые денежные суммы в высокой степени сконцентрированы у нескольких участников, финансовые последствия для остальных могут быть весьма существенными. Степень концентрации (т.е. доля, которая приходится на пять крупнейших участников), равная 80%, приводит к значительным проблемам для остальных участников системы. Кроме того, в системе нетто-расчетов финансовые обязательства участников, продолжающих их исполнять, существенны, если система достигает низкого неттинг-коэффициента[6], а участники имеют значительные дебетовые нетто-позиции. Финансовые последствия будут особенно серьезными в случае закрытия позиции. Следовательно, если розничные платежные системы обрабатывают даже относительно небольшие по сравнению с системами ВРРВ объемы платежей, к их оценке нужно подходить тщательно в случае достижения ими значительного неттинг-эффекта или номинальной суммы дебетовой нетто-позиции. Если неттинг-коэффициент системы составляет 10% или менее, а также если дебетовая нетто-позиция участников достигает по меньшей мере 1 млрд. евро, такой системе должно быть уделено пристальное внимание.

Если розничная платежная система занимает значительную долю рынка, обладает высокими совокупными финансовыми рисками и риском "эффекта домино", то это свидетельствует о ее системной значимости. В дополнение к этим общепринятым показателям центральные банки при осуществлении наблюдения за розничными платежными системами могут учитывать специфику конкретных рынков платежей. Ожидается, что по мере интеграции рынка платежей еврозоны и создания Единого пространства платежей в евро специфические национальные черты будут устранены.

2.2. Социально значимые розничные платежные системы

С точки зрения Евросистемы некоторые из "Ключевых принципов" настолько фундаментальны, что они должны быть обязательными не только для СиРПС, но также и для СоРПС еврозоны. В связи с этим Евросистема определила "Розничные стандарты", которым должны соответствовать СоРПС, если они играют важную роль в обработке и проведении розничных платежей, и сбой в которых может иметь серьезные экономические последствия и подорвать доверие населения к платежным системам и валюте в целом.

Степень финансовых рисков различна для СиРПС и СоРПС. По этой причине Евросистема считает, что те из "Ключевых принципов", которые касаются финансовых рисков (Принципы III—VI), не должны носить обязательный характер для СоРПС. Следовательно, при их идентификации Евросистема не будет фокусировать свое внимание на финансовых рисках, присущих системе, а скорее будет учитывать степень концентрации рынка розничных платежей и в особенности долю соответствующей системы на рынке. Доля, превышающая 25% платежей, обрабатываемых через межбанковские розничные платежные системы, а также на основе иных платежных соглашений, является показателем того, что система имеет социальную значимость.

Розничные платежные системы еврозоны, которые обязаны соответствовать "Розничным стандартам", всегда предоставляют клиринговые и расчетные услуги и в большинстве случаев принимают форму автоматизированной клиринговой палаты (АКП). В подобных системах платежные поручения, которыми обмениваются финансовые учреждения, АКП электронным способом сортирует и производит клиринг, а расчеты по ним осуществляет расчетный агент. В некоторых странах подобные инфраструктурные соглашения не обязательно принимают форму АКП, а могут представлять собой многосторонние межбанковские соглашения. Такие официальные и стандартизированные соглашения, основанные на частных договорах или на статутном праве, являются многосторонними и содержат свод общих правил.

Стандарты наблюдения Евросистемы применимы к системам типа АКП и многосторонним соглашениям. Между подобными системами, с одной стороны, и транзитными и двусторонними соглашениями — с другой должно проводиться различие. Транзитные соглашения объединяют несколько двусторонних соглашений. По причине того, что некоторые принципы (в частности, о доступе и управлении) носят слишком общий характер, чтобы быть применимыми напрямую к транзитным и двусторонним соглашениям, они не подпадают под действие "Розничных стандартов". Однако возможно, что в дальнейшем Евросистема установит специальные стандарты наблюдения для таких соглашений, включая корреспондентские банковские отношения и квазисистемы.

[6] Нетто-баланс взаиморасчетов — процентное отношение валового объема операций. Низкий неттинг-коэффициент указывает на высокий неттинг-эффект.

2.3. Прочие розничные платежные системы

Существуют и другие розничные платежные системы, которые не принадлежат ни к одной из двух вышеописанных категорий. Эти системы меньше воздействуют на финансовую инфраструктуру и экономику и, таким образом, им необязательно соответствовать “Ключевым принципам” или “Розничным стандартам”. Подобные системы должны отвечать специально установленным для них стандартам наблюдения, если таковые имеются. Примерами такого рода могут служить общие стандарты наблюдения за схемами с использованием электронных денег и другие национальные стандарты.

2.4. Дальнейшие действия

ЕЦБ и национальные банки по мере оценки значимости розничной платежной системы еврозоны устанавливают стандарты наблюдения. СиРПС подпадают под действие “Ключевых принципов”, СоРПС — под действие “Розничных стандартов”. К системам, не принадлежащим ни к одной из указанных категорий, применяются любые другие стандарты, например стандарты наблюдения за схемами с использованием электронных денег.

Евросистема сделает публичной информацию о том, какие розничные системы каким стандартам наблюдения должны отвечать, равно как и уже достигнутую степень соответствия стандартам. Системам, которые не в полной мере отвечают стандартам, придется предпринять надлежащие усилия для исправления ситуации. Разумеется, Евросистема также приветствует любые действия операторов систем, направленные на применение стандартов выше минимального уровня, а также дополнительных или всех “Ключевых принципов”, если они сочтут это уместным.

В рамках создания Единого европейского платежного пространства во многих розничных платежных системах еврозоны в настоящее время идут или планируются процессы консолидации или реформирования инфраструктуры. Евросистема будет принимать во внимание эти структурные изменения при оценке системы. Поэтому она будет требовать от системы, претерпевающей изменения, полного соблюдения стандартов наблюдения только в среднесрочной перспективе. Следовательно, система, которая находится в процессе реформирования или близка к завершению своей деятельности, до 2008 года будет регулироваться старыми положениями.

3. Применение “Ключевых принципов” к социально значимым розничным платежным системам еврозоны

В данной главе Евросистема кратко охарактеризует, почему те или иные “Ключевые принципы” должны или не должны применяться к СоРПС. В главе не разъясняются “Ключевые принципы” как таковые. Для более детального объяснения и интерпретации, пожалуйста, обратитесь к докладу “Ключевые принципы”, выходные данные которого приведены выше.

3.1. “Ключевые принципы”, которые должны соблюдать розничные платежные системы

Формулировка “Ключевых принципов” позволяет достаточно свободно их толковать и применять с учетом широкого круга обстоятельств. Таким образом, некоторые из “Ключевых принципов” не требуют столь же строгой их интерпретации в отношении СоРПС, как в отношении СиРПС. Следование соответствующему “Ключевому принципу” должно быть пропорционально степени значимости системы. Приведем два примера, призванных проиллюстрировать такой подход.

- Для того чтобы розничные платежные системы, не являющиеся системно значимыми, следовали Принципу I, не требуется обязательное независимое юридическое заключение для оценки юридической состоятельности системы. Сбор материалов для вынесения подобного заключения может быть ограничен специальной проверкой.
- Для того чтобы удовлетворять Принципу VII, безопасность и надежность функционирования СоРПС, а также соглашения на случай непредвиденных обстоятельств могут быть не такими, как для СиРПС.

Однако соответствующий орган наблюдения должен обеспечить, чтобы СоРПС соблюдали требования определенного "Ключевого принципа" с учетом всех обстоятельств в целом. В связи с этим Евросистема повторяет одно из положений доклада "Ключевые принципы", а именно о том, что основная ответственность за соблюдение соответствующих стандартов лежит на операторе рассматриваемой платежной системы. В своей оценке наблюдения того, как определенная розничная платежная система выполняет стандарты, Евросистема рассматривает более широкий круг вопросов, чем оператор, учитывая также последствия для экономики и финансовой системы в целом.

I. Правовой базис. Система должна иметь прочный правовой базис во всех юрисдикциях.
СоРПС должна обладать прочным правовым базисом. Если правила и процедуры системы неясны и не могут быть принудительно осуществлены согласно закону, то ее участники могут подвергнуться финансовым рискам.

II. Потенциальные финансовые риски. Правила и процедуры системы должны способствовать четкому пониманию участниками того, как система воздействует на все виды финансовых рисков, которым подвергаются ее участники.
Участники СоРПС должны оценивать риски, которым они подвергаются в такой системе. Им должно быть ясно, кто именно, в какой степени и какие конкретно риски несет. В значительной степени подобная информация должна быть отражена в правилах и процедурах, определяющих права и обязанности участников системы.

VII. Безопасность и надежность функционирования. Должны быть обеспечены безопасность и надежность функционирования системы, а также комплекс мероприятий на случай чрезвычайных обстоятельств, чтобы своевременно завершить дневной цикл работы системы.
Как финансовая экономика основана на использовании платежных систем, предназначенных для расчетов по финансовым сделкам, так реальная экономика в значительной мере зависит от работоспособности розничных платежных систем. Следовательно, СоРПС должна быть безопасна, надежна в работе, а также иметь комплекс мероприятий на случай чрезвычайных обстоятельств.

VIII. Эффективность: система должна предоставлять экономически эффективные и удобные для пользователей средства платежа.
Все СоРПС должны быть удобны для пользователей, а также экономически эффективны. Как правило, идет поиск баланса между снижением стоимости ресурсов и достижением других целей, например обеспечения безопасности. Разработчики платежных систем должны сокращать затраты, используя специфические условия системы и учитывая ее воздействие на экономику в целом. Там, где можно повысить общую эффективность розничных платежных систем еврозоны, особое внимание должно быть уделено внедрению в национальную розничную платежную систему международных стандартов (например, SWIFT, BIC, IBAN, IPI), которые позволят ускорить прямую обработку как национальных, так и международных операций.

IX. Критерии доступа: система должна иметь и публиковать объективные критерии участия, что позволит обеспечить справедливый и открытый доступ к ней.
Все СоРПС должны сформулировать и опубликовать объективные критерии участия. Критерии доступа, которые поощряют конкуренцию среди участников, способствуют предоставлению эффективных услуг более низкой стоимости. Таким образом, доступ должен быть в целом свободным и открытым. Тем не менее возможны некоторые ограничения доступа для защиты участников от чрезмерных рисков, которые возникают в результате участия других сторон.

X. Управление: структура управления системой должна быть эффективной, контролируемой и прозрачной.
Структура управления СоРПС должна быть эффективной, контролируемой и прозрачной. С помощью структуры управления устанавливаются и решаются общие задачи системы и ведется мониторинг ее деятельности. Такая структура должна надлежащим образом стимулировать менеджмент к достижению целей, которые соответствуют интересам системы, ее участников и государства в целом. Структура управления должна гарантировать подотчетность систем соответствующим органам и быть прозрачной, чтобы все заинтересованные стороны могли иметь доступ к необходимой информации.

3.2. Прочие "Ключевые принципы"

Перечисленные ниже "Ключевые принципы" не являются обязательными для СоРПС, но, как уже кратко излагалось выше, Евросистема приветствует применение операторами всего комплекса "Ключевых принципов", если они сочтут это уместным.

IV. Своевременное завершение расчетов: система должна обеспечивать своевременное завершение расчетов в течение дня (что предпочтительнее) или по крайней мере в конце дня.

Условия, наиболее оптимальные для розничных платежных систем еврозоны

В случае с системно значимыми платежными системами важно, чтобы окончательный расчет — то есть отнесение средств на дебет или кредит счетов участников — совершался в день расчета, предпочтительнее даже в течение дня, чтобы участники не подвергались чрезмерным кредитным рискам. При осуществлении крупных платежей или расчетов по операциям на финансовом рынке в целях управления риском участники должны твердо знать, что в течение или в конце расчетного дня будут произведены окончательные расчеты по подобным операциям. При осуществлении розничных платежей речь идет о меньших объемах средств, и в большинстве случаев получатели не придают такое же значение своевременности завершения расчетов. Так как Евросистема не требует от розничных платежных систем еврозоны строгого соблюдения Принципов III и V, что будет объяснено ниже, нет основания осуществлять расчет в день платежа и реализовывать меры, направленные на обеспечение своевременности его завершения даже в случае несостоятельности участника. Таким образом, окончательный расчет в день платежа не является обязательным для розничных платежных систем еврозоны.

Однако если розничные платежные системы не обеспечивают окончательный расчет в день платежа, период, в течение которого суммы участников подвергаются риску, может составлять несколько дней (например, включая выходные дни). Такого риска можно избежать в СоРПС, если окончательный расчет производится в день платежа[7]. Технологический прогресс предполагает, что свойства системы могут регулироваться на основе контроля затрат. Поэтому расчет в день платежа является условием, крайне желательным для СоРПС.

III. Управление финансовыми рисками: система должна обладать строго формализованными процедурами для управления кредитными рисками и рисками ликвидности, данные процедуры определяют ответственность оператора и участников системы, а также обеспечивают адекватные стимулы для управления и сдерживания таких рисков.

Средства управления рисками (например, залоговый фонд, дебетовые лимиты), несомненно, входят в комплекс безопасности платежной системы. Однако должен соблюдаться баланс между безопасностью и эффективностью. Поэтому совершенно ясно, что следует различать требования к безопасности розничных платежных систем и платежных систем для крупных сумм, так как различны степени риска в указанных системах. Операторы системы должны решить, какие инструменты управления рисками в наибольшей степени ей соответствуют.

V. Расчет в системах неттинга на многосторонней основе: системы, в которых используется многосторонний неттинг, по меньшей мере должны обеспечивать возможность своевременно завершать ежедневные расчеты в случае, если участник, обладающий самой большой нетто-позицией, не в состоянии этого сделать.

Как уже упоминалось выше, согласно Принципу III в каждой розничной платежной системе должен поддерживаться баланс между безопасностью и эффективностью. Если операторы системы считают уместным не включать средства управления рисками в свои розничные системы, существует риск того, что в случае неспособности одного из участников осуществить расчет система не сумеет завершить расчет за один день. Операторы должны изучить, как их система сможет обеспечить своевременное завершение расчетов в максимально возможном объеме, если произойдет сбой.

VI. Расчетные активы: желательно, чтобы используемые для расчетов активы представляли собой требования к центральному банку; в случае если используются другие активы, то они могут подвергаться незначительным кредитным рискам и незначительным рискам ликвидности или быть свободными от обоих.

Использование денежных средств центрального банка для расчетов позволяет не подвергать участников платежных систем кредитным рискам в случае дефолта расчетного агента. Таким образом, денежные средства центрального банка являются самым надежным активом для проведения расчетов. Так как розничные платежные системы, как правило, не имеют системной значимости, из-за низкой степени риска расчеты денежными средствами центрального банка при работе таких систем не требуются. Проведение расчетов через центральный банк осуществляется по усмотрению оператора системы, но если он решит использовать для расчета денежные средства коммерческого банка, такой коммерческий банк должен иметь соответствующий статус.

[7] Расчет в день платежа для розничных платежных систем не обязательно означает, что он должен произойти в день передачи платежных поручений в систему. В соответствии с этим принципом участники подвергаются кредитному риску (если расчет происходит через несколько дней) со времени передачи платежных поручений и до тех пор, пока средства не отнесены на дебет и кредит счетов.

4. Регистрация розничных платежных систем в соответствии с “Директивой о завершении расчетов” (ДЗР)

ДЗР придает юридическую силу исполнению платежных поручений и проведению неттинга на случай, если будет возбуждена процедура банкротства в отношении одного из участников системы. Поэтому Евросистема высоко оценивает тот факт, что согласно ДЗР все системно значимые платежные системы еврозоны являются субъектами регистрации. Более того, Евросистема придерживается мнения, что согласно ДЗР целесообразно регистрировать платежные системы, не являющиеся системно значимыми, в частности, социально значимые. Это подтверждает то, что регистрирующий орган при принятии решения о статусе подобной системы может учитывать национальные особенности.

Евросистема придерживается мнения, что из-за специфических характеристик розничных платежных систем весьма желательно проводить их регистрацию в соответствии с ДЗР. Широкое иностранное участие может привести к появлению в розничных платежных системах юридических рисков. Например, законодательство, регулирующее деятельность зарубежных участников, получающих доступ к системе через филиалы или дистанционно, может соответствовать применяемому к системе законодательству не полностью. Законодательство, регулирующее, например, залоги, неттинг, завершение расчетов или дела о несостоятельности и банкротстве, действующее в стране одного из участников, может отличаться от законов, действующих в другой стране, где платежная система осуществляет свою деятельность. По мнению Евросистемы, негативные последствия для платежной системы, возникающие из-за несостоятельности зарубежного участника, можно свести к минимуму в случае регистрации соответствующей системы согласно ДЗР. В подобных случаях права и обязанности участника в связи с его участием в системе будут определяться в рамках законодательства той страны, в чьей юрисдикции система находится. Еще одно преимущество регистрации состоит в том, что если судебные или административные органы (в том числе и зарубежные) принимают решение о начале процедуры банкротства в отношении одного из участников, система немедленно получит информацию об инициировании процедуры банкротства и сможет предпринять немедленные и надлежащие действия.

НАБЛЮДЕНИЕ ЗА ПЛАТЕЖНЫМИ СХЕМАМИ, ФУНКЦИОНИРУЮЩИМИ С ИСПОЛЬЗОВАНИЕМ КАРТ. СТАНДАРТЫ

Европейский центральный банк

Январь 2008 г.

Содержание

1. Введение*

Во многих европейских странах платежи, совершаемые с использованием карт, составляют большинство трансграничных розничных операций и являются наиболее распространенными платежами в сети Интернет. Статистические данные по еврозоне свидетельствуют о том, что за прошлые пять лет объем операций с использованием дебетовых и кредитных карт увеличился почти в два раза. В еврозоне основано более двадцати *платежных схем, функционирующих с использованием карт (ПСК),* однако рынок все еще раздроблен, поскольку большинство из схем являются национальными схемами на основе дебетовых карт. Рост использования карт повышает интерес центральных банков и рынка в целом к безопасности их обращения и развитию платежной инфраструктуры.

В соответствии со Статьей 105 (2) "Соглашения об учреждении Европейского экономического сообщества" и Статьями 3 и 22 "Устава Европейской системы центральных банков и Европейского центрального банка", одной из основных задач Евросистемы является содействие бесперебойному функционированию платежных систем. В связи с этим в заявлении Европейского центрального банка 2000 года определена роль Евросистемы в области наблюдения за платежными системами[1]. В частности, в этом документе говорится о том, что "Евросистема может также разработать политику в отношении безопасности платежных инструментов, чтобы сохранить доверие пользователей к платежным системам".

В соответствии с этими полномочиями Евросистема приняла решение разработать общую политику наблюдения, чтобы обеспечить надежность ПСК еврозоны, а также доверие общества к платежам с использованием карт и их одинаковые условия на всей территории еврозоны в рамках объединенного рынка. Наблюдение за ПСК основано на унифицированном и риск-ориентированном подходе, в частности, оно строится на детальном изучении рынка платежей, совершаемых с использованием карт, а также исследовании рисков, которым подвергаются ПСК. Настоящий документ построен следующим образом. Раздел 2 содержит отличительные особенности подхода по наблюдению. Разделы 3 и 4 характеризуют соответственно область применения и организации, которым адресованы подходы по наблюдению. Раздел 5 описывает политику освобождения от применения стандартов наблюдения и Раздел 6 разъясняет методологию. Раздел 7 содержит подробное описание стандартов наблюдения. Кроме того, в Приложении А представлена модель ПСК и в Приложении Б — глоссарий терминов.

2. Отличительные особенности подхода по наблюдению

Большинство центральных банков Европейского союза уже имеют и осуществляют политику наблюдения за ПСК в необходимой для поддержания безопасности мере, которая сохранит определенный уровень доверия к средствам платежа и в конечном итоге к деньгам. Более трех четвертей европейских центральных банков считает обеспечение эффективности ПСК частью своих функций. Тем не менее центральные банки не придерживаются единых стандартов или руководящих принципов. ПСК оценивается в соответствии с целым рядом стандартов, таких как "Ключевые принципы для системно значимых платежных систем"[2], лучшей практикой в сфере обеспечения безопасности и других областях или в соответствии с риск-ориентированным подходом. Подавляющее большинство центральных банков получают статистические данные и общую информацию о ПСК от самих ПСК или эмитентов карт. В некоторых случаях органы наблюдения обмениваются информацией о деятельности международных ПСК.

С учетом вышеизложенного цель данного исследования — сформулировать необходимый минимум стандартов в области наблюдения за ПСК на основе опыта, накопленного к настоящему времени. Данные стандарты в значительной степени аналогичны стандартам наблюдения за европейскими розничными платежными системами[3], а также учитывают необходимость обеспечить безопасность и эффективность ПСК. Стандарты наблюдения не зависят от каких-либо правовых или профессиональных правил, применяемых к ПСК.

---

* Данный материал является неофициальным переводом публикации ЕЦБ "Oversight framework for card payment schemes — standards" ("Наблюдение за платежными схемами, функционирующими с использованием карт. Стандарты"). Электронная версия данной публикации на английском языке размещена на веб-сайте ЕЦБ *(www.ecb.int/pub/pdf/other/oversightfwcardpaymentsss200801en.pdf).*

[1] ЕЦБ, "Роль Евросистемы в области наблюдения за платежными системами", 2000 год.

[2] Банк международных расчетов, "Ключевые принципы для системно значимых платежных систем" (так называемые "Ключевые принципы"), 2001 год.

[3] ЕЦБ, "Стандарты наблюдения за европейскими розничными платежными системами", 2003 год.

3. Область применения

Наблюдение должно распространяться на все ПСК, в том числе на трехсторонние и четырехсторонние, предоставляющие платежные услуги с использованием дебетовых и/или кредитных карт. Определение ПСК приведено в Блоке А. Наблюдение также распространяется на дебетовые предоплаченные карты и соответствующие счета. Однако к денежным средствам, которые хранятся непосредственно на предоплаченной карте, данный подход по наблюдению не применяется, поскольку такие карты подпадают под наблюдение Евросистемы за электронными деньгами.

4. Организации, которым адресованы подходы по наблюдению

Стандарты наблюдения разработаны для использования органами управления ПСК. Однако по согласованию с органом наблюдения орган управления может назначать уполномоченных участников, которые будут отвечать за определенные функции ПСК. В таких случаях разграничение ответственности между организациями должно быть четко сформулировано, прозрачно и официально оформлено.

5. Политика освобождения от применения стандартов наблюдения

Для того чтобы не сдерживать инновации, не усложнять деятельность малых ПСК и распределять усилия по наблюдению пропорционально рискам, допускается политика освобождения от применения стандартов наблюдения. Данная политика применяется в отношении европейских ПСК в контексте создания Единого пространства платежей в евро (SEPA) с учетом трансграничного характера использования карт в настоящее время, последствий сбоев в ПСК, которые сказываются на общественном доверии к картам, а также с учетом рисков, способных привести к потере денежных средств.

На ПСК не распространяются стандарты наблюдения, если схема удовлетворяет следующим критериям в пределах еврозоны:

а) в течение последних трех лет количество выпущенных карт составляет в среднем меньше 1 миллиона штук в год; или

б) в течение последних трех лет осуществлены операции со среднегодовым оборотом на сумму меньше 1 миллиарда евро.

Национальные центральные банки могут принять решение о применении более строгих правил в отношении ПСК, находящихся в их юрисдикции и имевших ранее право на освобождение. Это решение может быть обусловлено факторами риска и важностью ПСК в общенациональном контексте.

6. Методология

Стандарты наблюдения были разработаны с учетом характера рисков (см. ниже). Стандарты наблюдения за европейскими розничными платежными системами — логическая модель для стандартов, которая, однако, была адаптирована с учетом специфики ПСК и в которой учтены требования по безопасности и операционной деятельности. Основные особенности каждого из стандартов исследованы и объяснены в пояснительной записке, уделяющей большое внимание специфике ПСК.

6.1. Виды рисков

Анализ рисков проведен с целью определения активов, которые должны быть защищены, чтобы обеспечить бесперебойное функционирование ПСК. Эти активы подвержены различным видам рисков. Риски могут быть прямыми (например, изготовление поддельной карты) или являться следствием других рисков (потеря репу-

Блок А

Платежная схема, функционирующая с использованием карт (ПСК). Определение

В области наблюдения за платежными системами под платежной схемой, функционирующей с использованием карт, подразумевается набор функций (см. Приложение А), процедур, соглашений, правил и устройств, которые позволяют держателю *карты* совершать платежи и/или получать наличные деньги в инфраструктуре, созданной с участием не только эмитента карты, но и других учреждений. Наблюдение охватывает весь платежный цикл, то есть *операционную фазу* (включая совершение платежа и обработку данных), фазы клиринга и расчета, а также как сферу функционирования розничных платежных систем, так и сферу использования платежных инструментов.

тации учреждения в результате изготовления поддельной карты), и не все эти риски равнозначны. Тем не менее следует уделять должное внимание каждому из этих рисков, поскольку они способны прямо или косвенно влиять на безопасность и эффективность функционирования ПСК.

В любой платежной системе существуют правовые, операционные и финансовые риски. Значимость указанных рисков и их воздействие на бесперебойное функционирование платежной системы зависят от характера самой системы. Например, если платежная система является системно значимой, возникновение финансовых рисков негативно влияет на финансовую стабильность, в то время как на розничные платежные системы риски могут не оказать такое влияние. В большей или меньшей степени эти риски имеют место в ПСК. Несмотря на то что их возникновение может и не привести к системным финансовым нарушениям, как в случае с системно значимыми платежными системами, тем не менее они достаточно сильно воздействуют на систему в целом. Например, они, по крайней мере временно, значительно влияя на способность экономических агентов выполнять обязательства ввиду отсутствия и/или недостатка доверия к платежным картам и замещающим их платежным инструментам, способны нарушить деятельность реального сектора экономики. На практике серьезность последствий будет зависеть от рыночной структуры платежных услуг и, в частности, от значимости карт и других замещающих их платежных инструментов.

ПСК должна быть защищена от рисков на протяжении всего платежного цикла, а не только в клиринговой и расчетной фазе, и для этого требуются действующие и результативные механизмы управления. Неэффективность механизмов управления может быть причиной других видов рисков, поскольку эти механизмы не всегда применимы для таких видов рисков, как, например, операционный. Для решения проблем, вызванных рисками неэффективного управления, необходимо использовать общее управление рисками.

Кроме того, на ПСК риск потери репутации отражается больше, чем на других видах платежных систем. Потеря репутации серьезно сказывается на доверии к инструменту в целом, оправдывая свое название “репутационный риск”. Чаще всего репутационный риск возникает как результат других видов рисков (например, правового и операционного), но и вероятность прямого возникновения репутационного риска не исключена (например, в случае распространения ложной информации).

Стандарты наблюдения за ПСК уделяют большое внимание операционному риску по двум причинам. Во-первых, для эффективного функционирования ПСК снижение операционного риска имеет ключевое значение. Низкий уровень безопасности, операционной надежности и непрерывности бизнеса могут привести к потере общественного доверия к данному инструменту и, следовательно, нарушениям функционирования рынка. Во-вторых, управляя операционным риском, следует принимать во внимание специфику, разнообразие и комплексность ПСК, особенно технические аспекты и использование аутсорсинга, что подразумевает проведение углубленного анализа инфраструктуры ПСК.

6.2. Определение рисков

Правовой риск — риск убытков в связи с неожиданным применением закона или иного правового акта либо в связи с невозможностью добиться принудительного исполнения договора. Правовой риск возникает, если права и обязанности участников ПСК отличаются правовой неопределенностью. Анализ правовых рисков в ПСК является трудоемким вследствие сложности и разнообразия ПСК, которые включают различные этапы и взаимодействие разных задействованных лиц (например, *операторов, эмитентов, эквайреров, держателей и акцептантов карт).* Правовая база международных ПСК еще более сложная в связи с различиями в подходах регулирования, которые приходится учитывать, чтобы обеспечить правовую силу обязательств договора во всех соответствующих юрисдикциях.

Финансовый риск охватывает целый ряд рисков, возможных при совершении финансовых операций, включая риск ликвидности и кредитный риск. Стандарты наблюдения также направлены на снижение финансовых рис-

ков в ПСК, включая потенциальные потери от операционных рисков (например, мошенничества). Клиринговая и расчетная фазы в ПСК могут подвергаться финансовым рискам, связанным с невыполнением обязательств или банкротством расчетного агента или *провайдеров услуг.* В частности, эквайрер сталкивается с риском ликвидности или кредитным риском, если эмитент не в состоянии рассчитаться по обязательствам.

Риск общего управления, как правило, указывает на отсутствие политики регулирования и управления в ПСК и обычно возникает в случаях, когда обязанности участников должным образом не распределены и если решения, касающиеся целей и действий, разделяются не всеми участниками. Риск общего управления часто порождает другие риски (операционный, правовой и т.д.), поскольку он связан с базовыми функциями управления любой ПСК. Основными последствиями данного риска являются конфликт интересов участников и неспособность или нежелание поддерживать динамику развития рынка и инновации, а также принимать соответствующие меры в кризисных ситуациях. Этот риск способен существенно повлиять на конкуренцию, если политика доступа к схемам непрозрачна и неадекватна предъявляемым требованиям. Ненадлежащее распределение обязанностей может препятствовать некоторым участникам ПСК быстро и эффективно принимать соответствующие меры в кризисных ситуациях.

Операционный риск — результат нечетко выстроенных внутренних процессов и систем или сбоя в их работе, а также человеческой ошибки или внешнего воздействия на какой-либо из компонентов ПСК. Операционный риск возникает в результате невыполнения полностью одного или более этапов платежного процесса. Операционный риск включает риск мошенничества, который в соответствии с определением является неправомерным или преступным действием, способным привести одну из участвующих сторон к финансовым потерям, и который, вероятно, является следствием ненадлежащих мер безопасности. Типичный риск мошенничества — несанкционированное снятие средств со счета держателя карты.

Репутационный риск может быть определен как вероятность появления негативной информации о деятельности учреждения — возможно, и необоснованной, — которая влечет за собой сокращение клиентской базы, дорогостоящие судебные процессы, снижение доходов и ликвидности, а также существенное уменьшение рыночной капитализации. Поскольку клиенты склонны выбирать ПСК, основываясь на ее репутации и стоимости услуг, важно учитывать репутационный риск. Репутационный риск имеет отношение главным образом к брендменеджменту. Влияние репутационного риска трудно определить в количественном выражении и/или определить вообще, поскольку он является одновременно и самостоятельным, и производным риском, то есть обусловлен другими рисками и уязвимыми местами схемы. Потеря репутации неожиданно возникает в результате операционных сбоев или предоставления недостоверной или недостаточной информации конечным пользователям. Иными словами, как показывает практика, репутационный риск возникает в целом из-за кризисных ситуаций в других областях, однако после реализации репутационный риск становится значимым сам по себе и требует принятия особых мер.

7. Стандарты наблюдения

Исходя из вышеизложенного и принимая во внимание сведения, приведенные в Приложении А, были определены пять стандартов: правовые вопросы, прозрачность, операционная надежность, квалифицированное управление, надежные процессы клиринга и расчета. Иными словами, каждая ПСК должна:

1) располагать надежной правовой базой во всех соответствующих юрисдикциях;
2) предоставлять участникам полную информацию о своей деятельности, включая сведения о финансовых рисках;
3) обладать достаточным уровнем безопасности, операционной надежности и непрерывности бизнеса;
4) использовать эффективные, контролируемые и прозрачные механизмы системы управления;
5) управлять финансовыми рисками, возникающими в процессе клиринга и расчета.

Стандарт 1. ПСК должна располагать надежной правовой базой во всех соответствующих юрисдикциях

Ключевые вопросы

1.1. Правовые нормы, регулирующие создание и функционирование ПСК, а также взаимоотношения между ПСК и ее эмитентами, эквайрерами, *клиентами* и провайдерами услуг, должны быть полными, однозначными, современными, реалистичными и соответствовать действующему законодательству.

1.2. В случае регулирования ПСК в различных юрисдикциях действующее в них законодательство должно быть проанализировано с целью выявления противоречий между ними. Там, где противоречия есть, должны быть предприняты меры, направленные на смягчение их последствий.

Пояснительная записка

- Отсутствие соответствующего юридического оформления может сделать незаконными все правила и договоры, регулирующие ПСК и ее отношения со своими *участниками.*

  В случаях несоответствия требованиям действующего законодательства правила и/или договоры (или некоторые их части) будут недействительными, что может привести к неопределенности. Поэтому важно уделять должное внимание юридическим вопросам с самого начала. Именно на этапе учреждения ПСК закладываются основы ее устойчивого функционирования в будущем.

  В тех случаях, когда правовая база является надежной, правила и договоры — однозначными, все участники ПСК имеют четкое представление о своих правах и обязанностях. Это снижает вероятность рисков и расходов, возникающих вследствие неоднозначных юридических формулировок.

  Поскольку законы претерпевают изменения, отсутствие регулярного контроля за правовой средой, а также своевременной актуализации правил и договоров ПСК приводит к расхождениям между ними и действующим законодательством, что является причиной правовой неопределенности в отношении ПСК.

  Например, в связи с характером своей деятельности ПСК может столкнуться с риском, связанным с проверкой ее на соответствие требованиям в области конкуренции или защиты данных со стороны регулирующих органов. Концентрация таких рисков в конечном счете имеет серьезные последствия для участников ПСК.

- В случае если ПСК осуществляет свою деятельность на международном рынке, задача обеспечения правовой определенности усложняется. Именно поэтому очень важно, чтобы правила и договоры были приведены в соответствие с законодательством данной юрисдикции. В противном случае возможность осуществить правила и договоры ПСК в судебном порядке может быть оспорена.

Стандарт 2. ПСК должна предоставлять участникам полную информацию о своей деятельности, включая сведения о финансовых рисках

Ключевые вопросы

2.1. Все правила и договоры ПСК должны быть надлежащим образом оформлены и обновляться по мере необходимости. Все участники, включая потенциальных, должны иметь беспрепятственный доступ к необходимой им информации в той степени, которая разрешена законодательством о защите данных, чтобы они могли в случае необходимости предпринять надлежащие меры. Важные конфиденциальные сведения должны раскрываться только на основе принципа необходимого знания.

2.2. Эмитенты, эквайреры, держатели и акцептанты карт должны иметь доступ к соответствующей информации для оценки их финансовых рисков.

Пояснительная записка

- В отсутствие надлежащей документации (например, договоров) относительно ролей и обязанностей всех участников ПСК или надлежащего управления их взаимодействием может возникнуть риск общего управления. В ПСК это особенно актуально, так как операционный риск, в том числе риск мошенничества, приводит к финансовым потерям одной или нескольких сторон. Нехватка согласованной и актуальной информации, направленной на снижение риска мошенничества, например информации о способах обнаружения копирующих устройств и защиты ПИН, является причиной финансовых потерь и снижения доверия к платежным инструментам. Однако раскрытие важной конфиденциальной информации создает угрозу безопасности ПСК.

  Соответствующая документация по оценке возможных рисков, обусловленных участием в ПСК, должна быть также доступна для ее потенциальных участников.

- Если эмитенты, эквайреры, держатели и акцептанты карт не имеют доступа к информации о рисках, связанных с их участием в ПСК, то они сталкиваются с рисками в процессе клиринга и расчетов, а также рисками мошенничества и/или возврата денежных средств. Вследствие сложности ПСК участники могут оказаться не в состоянии выявить и оценить затрагивающие их интересы риски.

Стандарт 3. ПСК должна обладать достаточным уровнем безопасности, операционной надежности и непрерывности бизнеса

Ключевые вопросы

3.1. Управление безопасностью

3.1.1. Анализ операционных рисков и рисков безопасности следует проводить на регулярной основе, чтобы определить приемлемый уровень риска и выбрать соразмерную политику безопасности, а также определить соответствующие процедуры, чтобы предотвратить, обнаружить, ограничить и исправить нарушения в области безопасности. Соблюдение политики безопасности должно регулярно оцениваться.

3.1.2. Руководство и персонал должны быть надежными и компетентными (с точки зрения квалификации, профессиональной подготовки и количества сотрудников) в принятии соответствующих решений по поддержанию политики безопасности и выполнению своих обязанностей и функций, связанных с деятельностью ПСК.

3.1.3. Оперативное руководство и контроль происшествий в каждой конкретной ситуации должны быть четко определены и эффективны.

3.1.4. Политика безопасности ПСК должна обеспечивать конфиденциальность, *целостность* и *достоверность* данных, а также *безопасность секретной информации* (например, *ПИН*) при ее обработке, хранении и обмене. Если секретная информация раскрыта или ее безопасность скомпрометирована, должен быть реализован эффективный план ответных действий по защите ПСК.

3.2. Изготовление и распространение карт

3.2.1. При проектировании и производстве платежных карт, а также принимающих и других технических устройств необходимо обеспечить достаточный уровень безопасности в соответствии с политикой безопасности ПСК.

3.2.2. Эффективные и безопасные процедуры должны применяться при инициализации, персонализации и доставке карт держателям и доставке *принимающих устройств* акцептантам, а также при формировании и предоставлении секретной информации (например, *ПИН*).

3.3. Совершение операций

3.3.1. В соответствии с политикой безопасности ПСК следует применять адекватные стандарты безопасности при инициировании операций. Компоненты ПСК должны быть защищены от несанкционированного вмешательства. ПСК должна иметь возможность снизить риски, связанные с использованием платежных карт в сети без авторизации в режиме реального времени или с менее безопасными *аутентификационными* мерами (например, при совершении дистанционных платежей).

3.3.2. Необходимо постоянно осуществлять мониторинг деятельности держателей и акцептантов карт для того, чтобы своевременно реагировать на мошенничество и любые риски, сопровождающие их деятельность. Следует разработать меры, которые ограничат воздействие мошенничества.

3.3.3. Должны быть предприняты меры, которые обеспечат проведение операций с использованием карт в пиковое время и в пиковые дни.

3.3.4. Необходимо предоставить возможность получать достаточно доказательств, позволяющих открыто разрешать споры между участниками.

3.4. Клиринг и расчет

3.4.1. Процедуры клиринга и расчета должны учитывать предельные сроки расчетов, которые предусмотрены ПСК, и обеспечивать достаточный уровень безопасности, операционной надежности и доступности.

3.5. Непрерывность бизнеса

3.5.1. Анализ влияния бизнеса должен точно установить наиболее важные компоненты схемы для ее бесперебойного функционирования. В случае стихийного бедствия или любых других непредвиденных обстоятельств, угрожающих функционированию и доступности ПСК, должен быть реализован эффективный план действий по ее защите. Адекватность и эффективность таких планов должны быть проверены и регулярно пересматриваться.

3.6. Аутсорсинг

3.6.1. Рисками, которые возникают вследствие применения *аутсорсинга,* необходимо управлять на основе договоров. Договоры должны охватывать все вопросы, за которые отвечает участник, привлекающий партнеров на аутсорсинг для работ в ПСК.

3.6.2. Необходимо осуществлять управление и мониторинг деятельности партнеров по аутсорсингу. Привлекая партнеров на аутсорсинг, участники ПСК должны быть в состоянии подтвердить их соответствие стандартам, за выполнение которых они сами несут ответственность.

Пояснительная записка

Операционные риски, включая риски мошенничества, способны сильно повлиять на деятельность ПСК и подвергнуть опасности ее финансовую стабильность, что приведет одного или нескольких участников к финансовым потерям. Это может подорвать доверие пользователей к ПСК. Снижение этих рисков предполагает наличие мер, которые обеспечат следующее:

- надлежащее управление безопасностью;
- защищенность конфиденциальных данных или устройств при производстве и распространении карт;
- безопасность инициирования и проведения операций;
- безопасность и надежность клиринга и расчета;
- непрерывность бизнеса; а также
- контроль при аутсорсинге.

- **Надлежащее управление безопасностью**

  — Если ПСК нерегулярно проводит анализ операционных рисков и рисков безопасности с использованием широко распространенных и современных методик, это затрудняет разработку всесторонней политики безопасности. Отсутствие надлежащего управления рисками приводит к существованию таких стандартов безопасности, которые приемлемы по затратам, но не сокращают или не устраняют риски безопасности. Отсутствие надлежащего управления рисками приводит к появлению таких стандартов безопасности, которые приемлемы по затратам, но не сокращают или не устраняют риски безопасности. Управлять рисками невозможно, если система управления рисками не ориентирована на поддержку политики безопасности и не привержена ей.

  — Если квалификация или численность сотрудников недостаточны для того, чтобы справиться с возникающими проблемами безопасности, это нарушает бесперебойное функционирование ПСК. Недостаток знаний в области управления рисками и безопасности информационных технологий может привести к принятию ненадлежащих решений.

  — Инциденты в области безопасности происходят даже, когда, казалось бы, были приняты все необходимые меры. Бывает затруднительно сразу обнаружить причины указанных инцидентов или выявить уязвимость схемы. Это обусловлено неадекватными или недоработанными планами ответных действий по защите ПСК. Кроме того, в случае если не существует четкого и всестороннего понимания и оценки активов, то будет трудно определить последствия нарушения правил безопасности. Инциденты в области безопасности возникают в результате неспособности передать предупреждающие сообщения соответствующим получателям, поэтому последние не в состоянии должным образом отреагировать на уязвимость системы безопасности и мошенничество.

  — Кражи, подделки, сбои в работе, уничтожение, изменение и/или незаконное использование отдельных компонентов ПСК приводят к серьезным последствиям в области обеспечения безопасного функционирования схемы с точки зрения конфиденциальности, целостности и доступности. Такие события подвергают угрозе программное обеспечение, аппаратные средства или данные, необходимые для надлежащего функционирования ПСК (например, секретную информацию, технические и операционные параметры). Эти проблемы возникают, в частности, при проектировании и изготовлении компонентов ПСК, когда используются устаревшие стандарты безопасности и когда процедура их утверждения не регламентируется правилами, согласованными органом управления ПСК. Кроме того, деятельность ПСК подвержена влиянию других приложений, платежных схем и ПСК. Это происходит, например, когда несколько приложений включены в отдельный компонент ПСК (с точки зрения логического проектирования и технических особенностей безопасности). Секретная информация (например, *ПИН*) может быть раскрыта или скомпрометирована и использоваться для копирования компонентов схемы, чтобы совершить мошеннические операции, если данными компонентами не будут управлять должным образом и хорошо защищать их конфиденциальность.

- **Защита конфиденциальных данных или устройств при производстве и распространении карт, а также принимающих и других устройств**

  — Четкое и полное представление о специальных стандартах безопасности при проектировании и изготовлении карт, принимающих и других устройств имеет большое значение для борьбы с мошенничеством и хищением конфиденциальных данных. Важно, чтобы эти стандарты безопасности были основаны на политике безопасности ПСК и соответствовали ей, в противном случае могут быть реализованы ненадлежащие или неуместные меры безопасности.

  — Персональные данные, секретная информация (например, *ПИН*), карты или их реквизиты могут быть украдены (например, номера карт перехвачены в сети Интернет) или скомпрометированы и использоваться для осуществления мошеннических операций, если инициализация или персонализация компонентов ПСК недостаточна или отсутствует. Если оба процесса — выдача карты держателю и *доставка принимающих устройств* (терминалов, банкоматов и т.д.) — недостаточно защищены от кражи и незаконного присвоения, существует риск мошенничества.

- **Безопасное инициирование и совершение операций**

  — Если такие меры безопасности, как методы *аутентификации* являются недостаточными или отсутствуют, операции могут быть инициированы мошенническим путем. Это происходит, когда персональные данные, секретная информация (например, *ПИН*), карты или их реквизиты украдены (например, номер и другие реквизиты карты, перехваченные в сети Интернет) или скомпрометированы. Похищенная информация также используется для изготовления поддельных документов, открытия счета в банке или получения других платежных карт. Если лица, не имеющие на это полномочий, совершают указанные действия, то возникает угроза конфиденциальности, неприкосновенности частной жизни, доступности и целостности данных, а также риск раскрытия секретной информации. Кроме того, возникают риски от преднамеренных действий или непреднамеренных некорректных действий, повлекших за собой несанкционированное проникновение в помещения с ограниченным доступом (например, помещения, где хранится секретная информация) или подключение к конфиденциальным приложениям (например, серверам авторизации). Если ПСК позволяет инициировать операции в режиме реального времени без безопасной *авторизации* (например, *без использования карты*), мошенники могут легко воспользоваться такими ситуациями, если отсутствуют соответствующие меры безопасности или ограничений.

  — Без надлежащих мер по обеспечению безопасности, а также эффективного контроля за деятельностью держателей и акцептантов карт затруднительно ограничивать влияние мошеннических действий. Поэтому такие меры, как ведение списков аннулированных карт, возможность быстрого изменения секретной информации, операционные лимиты и т.д. могут быть реализованы в соответствии с политикой безопасности для снижения указанных выше рисков.

  — Каждый компонент ПСК способен обрабатывать или хранить определенное количество данных. Если этот предел достигнут, в пиковые часы или дни возможны проблемы доступности и целостности данных в ПСК.

  — Споры между участниками трудно регулировать при отсутствии прозрачной и доступной доказательной информации. Доверие к ПСК ставится под угрозу в случае частого повторения таких ситуаций.

- **Безопасный клиринг и расчет**

  — Проблемы в процессах клиринга и расчета могут привести к финансовым потерям, особенно держателей и/или акцептантов карт. Это происходит по причине несоответствия системы требованиям, предъявляемым к операционной надежности, безопасности и непрерывности бизнеса. Надлежащие уровни безопасности, операционной надежности и доступности в соответствии с уровнем риска и договорными обязательствами (например, расчетным периодом) имеют большое значение для обеспечения целостности всех данных, которыми обмениваются участники ПСК при проведении клиринга и расчета.

- **Непрерывность бизнеса**

  — Стихийные бедствия или значительные события, затрагивающие критически важные бизнес-процессы, могут надолго сделать ПСК непригодными. Если планы по обеспечению непрерывности бизнеса отсутствуют или недостаточно проработаны, то вследствие нарушения конфиденциальности и целостности информации и доступности сервисов ПСК возможны проблемы, ведущие к финансовым потерям.

- **Контроль при аутсорсинге**

— Если какие-либо функции ПСК осуществляются сторонними организациями, соглашения об уровне сервиса могут быть неполными и/или не обеспечивать контроль за предоставлением услуг, что в конечном итоге приводит к нарушению безопасности. Например, соглашения с подробным описанием уровня сервиса и штрафных санкций в случае мошенничества, процессинговых ошибок или недоступности услуг способствуют надлежащему управлению при аутсорсинге.

— Концентрация деятельности среди ограниченного числа партнеров по аутсорсингу создает серьезные проблемы в области обеспечения доступности и независимости ПСК.

Стандарт 4. ПСК должна использовать эффективные, контролируемые и прозрачные механизмы системы управления

Ключевые вопросы

4.1. Осуществляемые процессы можно определить как эффективные и прозрачные, когда:

— принимаются решения о целях бизнеса и политике доступа, включая политику доступа для эмитентов и эквайреров;

— анализируются эффективность, удобство и простота использования ПСК;

— выявляются риски, а также принимаются меры с целью уменьшить влияние этих рисков на бизнес.

4.2. Необходима эффективная система внутреннего контроля, включая независимый аудит.

Пояснительная записка

- ПСК обладают широким кругом заинтересованных лиц, включая эмитентов, эквайреров, держателей и акцептантов карт.

  — Адекватные и прозрачные механизмы управления имеют большое значение для принятия взвешенных решений, удовлетворяющих всех участников ПСК. Например, прозрачность политики доступа способствует пониманию участниками и клиентами вопросов, касающихся функционирования ПСК, а также рисков, с которыми они сталкиваются. Эти механизмы также помогают ПСК следовать за развитием рынка и инновациями, управлять конфликтами интересов, которые возникают в связи с участием широкого круга заинтересованных лиц, а также быстро и эффективно принимать меры в кризисных ситуациях. Столь же важно установить справедливые критерии входа и выхода на рынок, чтобы обеспечить прозрачность бизнеса. Это особенно касается случаев, когда на рынке возникают трудности и недостаточно альтернатив.

  — Бесперебойное функционирование ПСК с точки зрения клиента выражается в доступности ее сервисов. Обеспечение доступности сервисов ПСК — их управления, оценки и прогнозирования развития операционных потоков — является существенным для обеспечения работоспособности схемы в пиковые время и дни. Если орган управления ПСК не в состоянии собрать и проанализировать представленную клиентами в явной или неявной форме информацию о том, насколько схема удовлетворяет их стандартам, то потребности и ожидания клиентов могут оказаться неудовлетворенными. Это также может явиться причиной споров между участниками и/или проблем, обусловленных плохими результатами работы. Должное внимание к этим аспектам поможет сохранить доверие клиентов к ПСК.

  — Эффективные процессы управления рисками способствуют их выявлению, предотвращению и принятию соответствующих мер в случае необходимости. Эффективное управление рисками должно надлежащим образом учитывать риски, возникающие в условиях быстрого развития научно-технического прогресса, изменения ожиданий клиентов, распространения угроз, а также по мере выявления уязвимостей системы. Кроме того, оно дает возможность выявить наиболее существенные риски и информировать о них высшее руководство.

- Эффективные процессы внутреннего контроля важны для предотвращения и своевременного выявления сбоев и случаев мошенничества, приводящих к утрате доверия к ПСК. Обзор внутренних процессов должен обеспечивать оперативное выявление причин ошибок, мошенничества и несогласованностей, а также способствовать принятию восстановительных мер. Регулярный независимый аудит даст дополнительную уверенность относительно надежности принятых мер.

Стандарт 5. ПСК должна управлять финансовыми рисками, возникающими в процессе клиринга и расчета

Ключевые вопросы

5.1. ПСК должна выявлять финансовые риски в процессе клиринга и расчета, а также определять способы их устранения.

5.2. ПСК должна быть уверена, что провайдеры клиринговых и расчетных услуг имеют достаточную кредитоспособность, операционную надежность и безопасность.

5.3. Если существуют соглашения о завершении расчета в случае, когда эмитент не способен выполнять свои обязательства, должна быть уверенность в том, что в результате операции не будут превышены его возможности, в противном случае это поставит под угрозу его платежеспособность. ПСК должна также обеспечить, чтобы участники были в полном объеме осведомлены о своих обязательствах в рамках любого такого соглашения — в соответствии со Стандартом 2.

Пояснительная записка

- Завершение расчетов по операциям с использованием карт и финансовая стабильность ПСК могут быть поставлены под угрозу, если органом управления ПСК не оценены — и не уменьшены в случае необходимости — соответствующие финансовые риски, возникающие в процессе клиринга и расчета. В странах, где процессы клиринга и расчета в платежных системах находятся в сфере наблюдения центрального банка, орган управления ПСК может использовать этот факт при оценке риска.
- Неисполнение финансовых обязательств, операционный сбой или сбой в системе безопасности расчетного агента могут привести к существенным, хотя и не системным потерям. На это следует обратить внимание в том случае, если орган управления ПСК или ее участники располагают положительными балансами при расчетах с расчетным агентом. Поэтому необходимо, чтобы орган управления ПСК регулярно отслеживал кредитоспособность, операционную надежность и безопасность провайдеров клиринговых и расчетных услуг и был уверен, что заключенные с ними соглашения содержат положения о досрочном завершении процессов клиринга и расчета.
- Также могут существовать соглашения о завершении расчетов в случае, когда эмитент не способен выполнять свои обязательства, что необходимо для ограничения кредитного риска и риска ликвидности. Это может быть полезно как для снижения, так и для точности понимания финансовых рисков всеми участниками, особенно в системах с многосторонним неттингом, где расчеты могут быть приостановлены и/или возникнет неожиданная нехватка ликвидности.

Приложение А
Обзор платежных схем, функционирующих с использованием карт

ПСК включают в себя следующие подсистемы:

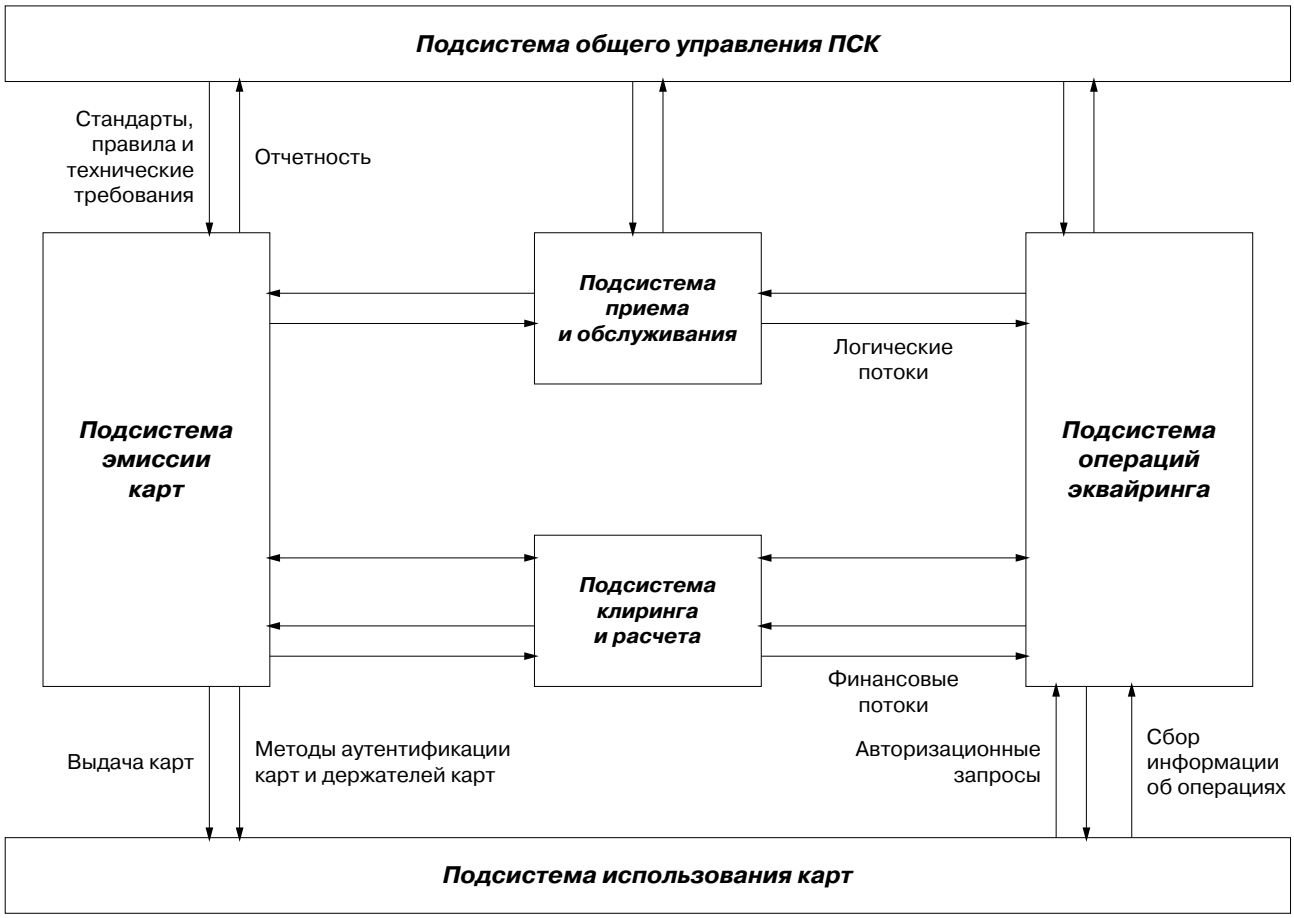
- общее управление;
- эмиссия карт;
- использование карт;
- эквайринг;
- услуги для обеспечения *приема* и проведения операций; а также
- клиринг и расчет.

Различные подсистемы, существующие в любой ПСК, представлены ниже (см. схему). Подсистемы классифицированы исходя из выполняемых ими задач, а не физических элементов (устройств) или организаций, отвечающих за их функционирование. Необходимо уточнить, что в рамках каждой подсистемы несколько организаций могут выполнять связанные задачи, например, в подсистему эмиссии карт вовлечены не только эмитенты карт.

Подсистема общего управления выполняет такие бизнес-функции, как, например, определение стандартов, правил и технических требований или отбор и утверждение уже существующих политик доступа, конкуренции, ценообразования, предотвращения мошенничества, управления и т.д.

Подсистема эмиссии карт взаимодействует с держателем карты и управляет данным процессом, отвечает за изготовление и персонализацию карты, обработку данных, подготовку ответов на аутентификационные и авторизационные запросы. Мероприятия, связанные с эмиссией карт, осуществляются эмитентами карт и сторонними провайдерами услуг, которым делегированы соответствующие полномочия.

Платежная схема, функционирующая с использованием карт



Подсистема использования карт отвечает за использование карты держателем, когда он осуществляет платеж акцептанту, и включает в себя все функции, необходимые для проведения операции в процессе *приема* карты (аутентификацию карты и/или держателя карты, запросы на авторизацию операции).

Подсистема операций эквайринга управляет акцептантами карт, обрабатывает и отправляет аутентификационные и авторизационные запросы, информацию о принятых операциях, а также управляет терминалами, включая их производство. Мероприятия, связанные с эквайрингом карт, выполняются как эквайрерами, так и сторонними провайдерами услуг, которым делегированы соответствующие полномочия.

Подсистема приема и обслуживания операций состоит из технических элементов, позволяющих осуществлять процесс *приема* карт и обмен информацией об операциях между подсистемами.

Подсистема клиринга и расчета отвечает за операции и инфраструктуру, необходимые для двустороннего или многостороннего клиринга и расчета по операциям с картами.

Приложение Б
Глоссарий терминов

Авторизация (authorisation): инициируемый с помощью терминала или банкомата процесс, посредством которого формируется распоряжение о переводе денежных средств держателем карты в пользу ее акцептанта. Данное распоряжение может быть одобрено или отклонено. В целом решение одобрить или отклонить операцию принимается эмитентом или третьей стороной от имени эмитента.

Акцептант карты (card acceptor): розничная торговая компания или любая другая организация, фирма или корпорация, заключившие соглашение с эквайрером для обеспечения приема карт при их предъявлении в качестве оплаты за товары и услуги (а также для снятия наличных средств), что в конечном итоге подразумевает перевод денежных средств в ее пользу.

Аутентификация (authentication): методы, используемые для проверки происхождения сообщения либо для проверки идентичности участника, подключенного к системе.

Аутентичность (authenticity): обеспечение идентичности предмета или ресурса заявленным параметрам. Понятие аутентичности применимо к пользователям, процессам, системам и информации.

Аутсорсинг (outsourcing): положение, когда провайдер услуг привлекает по договору третью сторону для выполнения своих обязанностей в ПСК. Каждый провайдер несет полную ответственность за осуществляемую за него деятельность по договору об аутсорсинге. Провайдер услуг должен обеспечить, чтобы все работы по аутсорсингу управлялись и контролировались так, как будто они были выполнены им самостоятельно.

Держатель карты (cardholder): физическое или юридическое лицо, которое заключает договор с эмитентом на получение платежной карты. Согласно договору держатель карты имеет право ее использовать в своих целях (например, для гарантии платежа, снятия наличных, гарантии чека, идентификации и др.).

Клиенты ПСК (customers of CPSs): участники — держатель и акцептант карты, — использующие услуги ПСК.

Конфиденциальность (confidentiality): свойство защищенности от несанкционированного раскрытия.

Криптографический алгоритм (cryptographic algorithm): математическая функция, используемая в сочетании с ключом, который обеспечивает конфиденциальность, целостность и/или аутентификацию данных. Криптографический алгоритм, использующий ключи, может быть симметричным или асимметричным. В симметричном алгоритме один ключ используется как для шифрования, так и для дешифрования. В асимметричном алгоритме для шифрования и дешифрования используются разные ключи. См. также *криптографический ключ.*

Криптографический ключ (cryptographic key): математическое значение, используемое в алгоритме шифрования или дешифрования текста. См. также *криптографический алгоритм.*

Маршрутизатор (switch): центр маршрутизации, который передает получателям запросы на авторизацию, полученные подтверждения и информацию об операциях.

Орган управления (governance authority): участник ПСК, который несет ответственность за ее общее функционирование и согласованность действий. Этот орган должен обеспечивать соблюдение всеми другими участниками установленных правил и в случае необходимости принять соответствующие меры. Стандарты предназначены именно для органов управления. Однако согласно правилам ПСК некоторые обязанности могут быть делегированы другим участникам ПСК. Орган управления должен четко регламентировать такие возможности и обеспечивать, чтобы выбор других участников ПСК соответствовал общим стандартам ПСК. Управляющим органом может быть специализированная организация или органы, ответственные за принятие управленческих решений в других взаимодействующих схемах.

Онлайн операция (on-line transaction): операция, одобрение или отклонение которой принимающим устройством происходит на основе взаимодействия между эквайрером и эмитентом карты (или его агентом) в режиме реального времени. Для этого необходимо, чтобы принимающее устройство было подключено к эквайреру в режиме реального времени во время проведения операции для отправки запроса и получения ответа.

Операционная фаза (transaction phase): эта фаза включает в себя подтверждение и авторизацию операции, а также процесс обмена данными, которые являются основанием для клиринга и расчета.

Офлайн операция (off-line transaction): обработка операции, ее одобрение или отклонение *принимающим устройством* на основе взаимодействия между ним и картой без фактической связи с эмитентом карты (или его агентом).

Платеж, совершаемый при отсутствии карты (card-not-present payment): операция, основанная на использовании реквизитов карты без ее физического предъявления торговой организации, например, при заказе товаров по почте, телефону, в сети Интернет.

Платежная схема, функционирующая с использованием карт (card payment scheme): в области наблюдения платежная схема, функционирующая с использованием карт, представляет собой набор функций, процедур, соглашений, правил и устройств, которые позволяют держателю карты совершать платежи и/или получать наличные деньги в инфраструктуре, созданной с участием не только эмитента карты, но и других учреждений. Наблюдение охватывает весь платежный цикл, то есть операционную фазу (включая совершение платежа и обработку данных), фазы клиринга и расчета, а также вопросы, связанные как с функционированием розничных платежных систем, так и с использованием платежных инструментов.

Прием (acceptance): процесс, при котором проверяется соответствие операции правилам ПСК (например, не истек ли срок действия карты или не подлежит ли карта изъятию; идентичны ли карта и ее держатель; не превышены ли финансовые лимиты владельца карты).

Платежная карта (payment card): устройство, позволяющее держателю карты проводить платежи за товары и услуги, как в любом устройстве приема, так и удаленно (например, при заказе товаров по почте, телефону, сети Интернет — известных как платежи без использования карты) либо получать наличные деньги в банкомате.

ПИН — персональный идентификационный номер (PIN — personal identification number): секретный код, используемый для проведения идентификации держателя карты (в ПСК главным образом используется четырехзначное число).

Персонализация карты (personalisation of a card): загрузка информации о клиенте, которая необходима при использовании карты для оплаты услуг и получения наличных денег.

Провайдер услуг (service provider): участники, обладающие внутренними или внешними ресурсами для оказания услуг клиентам ПСК. Провайдеры услуг включают: эмитентов, производителей карт, эквайреров, изготовителей терминалов, операторов служб поддержки, *маршрутизаторов* (организации, направляющие далее информацию об операциях), операторов, обслуживающих коммуникационные сети, а также операторов клиринговых и расчетных услуг. В некоторых случаях участник выполняет различные функции: например, в трехсторонней схеме эмитент и эквайрер совпадают. Учитывая значимость эмиссии и эквайринга в ПСК, в данном документе “эмитент” и “эквайрер” часто называются “участниками”.

Секретная информация (secret): информация, которая для соблюдения политики безопасности может быть известна только авторизованным пользователям.

Терминал (terminal): тип принимающего устройства.

Устройство приема (accepting device): устройство, обрабатывающее операцию, которая совершается с использованием платежной карты в присутствии ее держателя.

Участники ПСК (actors of a CPS): органы управления, провайдеры услуг, поставщики и клиенты (акцептанты и держатели карт).

Целостность (integrity): способность защититься от случайного или умышленного изменения или оповестить о произошедших изменениях.

Эквайрер карты (card acquirer): кредитная организация или провайдер платежных услуг, как они определены в “Директиве 2007/64/ЕС Европейского парламента и Совета ЕС” от 13 ноября 2007 года о платежных услугах на внутреннем рынке, а также другие организации, вступающие в договорные отношения с акцептантом и эмитентом карты посредством ПСК в целях обеспечения приема карт и обработки операций с их использованием. В некоторых случаях эквайрер карты является акцептантом карты.

Эмбоссирование (embossed): нанесение рельефных символов на поверхность карты.

Эмитент карты (card issuer): кредитная или в более редких случаях другая организация — участник ПСК, заключившая договор с держателем карты для ее обслуживания и использования в данной схеме.

НАБЛЮДЕНИЕ ЗА СИСТЕМАМИ ПРЯМОГО ДЕБЕТА. СТАНДАРТЫ

Европейский центральный банк

Август 2009 г.

Содержание

1. Введение*

У центральных банков есть четко поставленная цель — укрепление финансовой стабильности и обеспечение надежности платежных и расчетных систем. Согласно Статье 105 (2) "Соглашения об учреждении Европейского экономического сообщества" и Статьям 3 и 22 "Устава Европейской системы центральных банков и Европейского центрального банка" одна из основных задач Евросистемы заключается в "обеспечении бесперебойной работы платежных систем".

В феврале 2009 года Евросистема приняла решение дать более точное определение своей функции наблюдения и опубликовала новый документ о политике в области наблюдения[1]. В нем приводится общее представление о наборе механизмов и инструментов, применяемых Евросистемой, и подчеркивается, что платежные инструменты являются важным элементом платежных систем. Риски, связанные с предоставлением и использованием платежных инструментов, в основном не рассматриваются как системные, но безопасность и эффективность платежных инструментов необходимы, чтобы поддерживать доверие к денежному обращению и обеспечивать эффективность экономики.

Создание Единого пространства платежей в евро (SEPA) существенно меняет ситуацию с розничными платежами и повышает значимость согласованного подхода к наблюдению за платежными инструментами. Вследствие этого Евросистема разработала обобщенный подход и минимальный набор общих стандартов наблюдения за платежными инструментами, которые описаны в документе "Унифицированный подход и стандарты наблюдения за платежными инструментами" (ЕЦБ, февраль 2009 года). Цель этих стандартов — создать универсальную основу для наблюдения за всеми платежными инструментами, достаточно гибко подходя к особенностям отдельных инструментов. Данные стандарты закладывают фундамент для развития наблюдения за схемами прямого дебета и кредитовыми переводами в SEPA, а также для новых платежных инструментов, используемых в SEPA. Более того, каждый национальный центральный банк может также при необходимости применять общие стандарты при осуществлении наблюдения за другими национальными (не используемыми в SEPA) платежными инструментами. Чтобы учесть специфику каждого платежного инструмента, к которому применяются общие стандарты наблюдения, содержание каждого шага, предусмотренного унифицированным подходом Евросистемы к наблюдению за платежными инструментами, необходимо по-разному адаптировать для учета особенностей анализируемого платежного инструмента.

Данная методика наблюдения за системами прямого дебета использует соответствующие определения, содержащиеся в "Директиве 2007/64/ЕС Европейского парламента и Совета ЕС" от 13 ноября 2007 года о платежных услугах на внутреннем рынке (далее — "Директива о платежных услугах", или "PSD"). Так, прямой дебет определяется как "услуга по дебетованию платежного счета плательщика, когда сделка инициирована получателем платежа с согласия плательщика, которое он дал получателю платежа, провайдеру получателя платежа или провайдеру плательщика"[2]. Другие термины, использованные в настоящем документе, приведены в "Глоссарии терминов и определений" (Приложение Б).

Методика наблюдения базируется на использовании принципа декомпозиции и риск-ориентированного подхода, учитывающего, в частности, условия функционирования рынка платежей прямого дебета и управляющего соответствующими рисками, которым подвержены системы прямого дебета на протяжении всего платежного цикла, включая клиринг и расчет.

Цель наблюдения за системами прямого дебета — обеспечить надежность и эффективность платежей с помощью этих инструментов. Системы прямого дебета могут быть подвержены различным рискам, как любая платежная система. Они должны быть защищены от всех рисков, которые могут оказать всеобъемлющее влияние на доверие пользователей к данному инструменту. Следует четко разграничить проблемы системного характера (например, нарушение общепринятых правил или стандартов безопасности, которое подвергнет риску всех или большинство участников) и проблемы отдельных участников (например, неплатежеспособность одного из них, которая преодолевается в рамках банковского надзора) или проблемы, остроту которых надлежит смягчить отдельному участнику. Кроме того, особенно важно создать эффективные механизмы управления, а также помнить о необходимости предотвратить любой ущерб, угрожающий репутации используемого инструмента.

Данный документ построен следующим образом: Раздел 2 характеризует структуру стандартов по наблюдению; Раздел 3 обобщает различные риски, которым подвергаются участники системы прямого дебета; Раздел 4 дает представление об области применения методики; в Разделе 5 определены пользователи стандар-

---

* Данный материал является неофициальным переводом публикации ЕЦБ "Oversight framework for direct debit schemes" ("Методика наблюдения за системами прямого дебета"). Электронная версия данной публикации на английском языке размещена на веб-сайте ЕЦБ *(http://www.ecb.int/pub/pdf/other/oversightframeworkdirectdebitschemesen.pdf).*

[1] ЕЦБ, "Основы политики наблюдения Евросистемы", 2009 год.

[2] Определение дано в заголовке 1 Статьи 4 (28) "Директивы о платежных услугах".

тов; в Разделе 6 описаны сами стандарты. В Приложениях представлены обзор систем прямого дебета и глоссарий терминов.

Система прямого дебета (определение)

Согласно определению платежа прямого дебета PSD система прямого дебета может рассматриваться как набор функций (см. Приложение A), процедур, механизмов, правил и элементов, позволяющих осуществлять санкционированное дебетование платежного счета плательщика, инициированное получателем платежа в виде отдельного платежа или серии платежей. Методика наблюдения охватывает весь платежный цикл, то есть доступ к системе, стадию инициирования, стадию сделки, а также клиринг и расчет. Она учитывает вопросы, касающиеся как системы розничных платежей, так и используемых платежных инструментов.

2. Структура стандартов

Методика наблюдения следует "Унифицированному подходу и стандартам наблюдения за платежными инструментами" Евросистемы[3]. Общепринятые стандарты были разработаны на основе выявленных типов рисков (см. Раздел 3). Методика учитывает специфику систем прямого дебета, в частности, обусловленную особенностями операционной деятельности и обеспечения безопасности.

Каждый общепринятый стандарт наблюдения содержит ряд ключевых вопросов, которые рассмотрены и разъяснены в пояснительных записках.

3. Типы рисков

Участники системы (плательщик, получатель платежа, провайдер плательщика и провайдер получателя платежа) могут подвергаться определенным рискам. Платеж может быть возвращен, аннулирован или не исполнен по различным причинам, например, из-за мошенничества, операционных сбоев или финансового положения одного из участников. Для систем прямого дебета выявлены различные риски, в частности, правовой, операционный, репутационный или связанный с общим управлением.

Правовой риск относится к риску убытков, которые возникли в результате неожиданного применения закона или правовой нормы или невозможности добиться исполнения договора. Правовой риск возникает в связи с правовой неопределенностью в области реализации прав и обязанностей сторон, вовлеченных в систему прямого дебета. Анализ правовых рисков в системе прямого дебета затруднителен в силу сложности и разнообразия данной системы, предусматривающей многоэтапность процесса использования прямого дебета и многообразие участников (например, плательщика, провайдера плательщика, получателя платежа, провайдера получателя платежа, провайдеров услуг, а также клиринговые и расчетные механизмы). Правовая структура международной системы прямого дебета является еще более сложной, поскольку должна учитывать требования различных регулирующих систем для обеспечения ее правомочности в условиях соответствующих юрисдикций.

Финансовый риск охватывает ряд возникающих при финансовых сделках рисков, включая риск ликвидности и кредитный риск. Стандарты наблюдения призваны понизить уровень финансовых рисков, в т.ч. потенциальные убытки, обусловленные операционным риском (например, риском мошенничества). В рамках системы прямого дебета финансовые риски могут возникать у всех участников, получателей платежей, плательщиков и провайдеров платежных услуг. На стадии клиринга и расчета в системе прямого дебета финансовые риски могут быть вызваны дефолтом или неплатежеспособностью расчетного агента или провайдеров услуг. Для систем прямого дебета характерен финансовый риск, обусловленный плохим управлением разрешениями (мандатами, см. Глоссарий).

Операционный риск возникает в результате неадекватных или давших сбой внутренних процессов или систем, ошибок персонала, эксплуатирующего систему, или внешних событий, повлиявших на любой элемент системы прямого дебета[4]. Операционный риск может быть вызван неспособностью исполнить или завершить одну

[3] ЕЦБ, "Унифицированный подход и стандарты наблюдения за платежными инструментами", 2009 год.

[4] Банк международных расчетов, переработанное издание "Надежные практики управления и наблюдения за операционным риском", 2002 год; Банк Канады, "Working Papers", 2003, p. 11.

или несколько стадий платежного процесса. Операционный риск часто связан с доступностью системы прямого дебета.

Операционный риск включает риск мошенничества, определяемый как злонамеренный, или преступный, обман, который может привести к финансовым потерям одной из сторон, вовлеченных в сделку, и который, возможно, отражает неадекватные механизмы безопасности. Типичный риск мошенничества представляет собой несанкционированное дебетование платежного счета, которое способно повлиять на положение отдельных плательщиков. Возникновение некоторых рисков мошенничества обусловлено определенными технологическими решениями, например, спецификой маршрутизации разрешений и верификацией операций прямого дебета.

Репутационный риск можно определить как вероятность обоснованного или необоснованного ухудшения репутации системы, которое приводит к сокращению клиентской базы, затратным судебным процессам, снижению доходов, проблемам с ликвидностью или значительному уменьшению рыночной капитализации. Сложность системы прямого дебета и высокий уровень автоматизации операционных процессов затрудняют понимание клиентами нюансов ее работы. Однако системы прямого дебета, как правило, тесно связаны с автоматизированными системами конечных бизнес-пользователей, которые способны оценить, насколько определенная система прямого дебета может удовлетворить их операционные потребности. Это наряду с репутацией и стоимостью услуг является для конечных пользователей важным параметром при выборе системы. Репутационный риск плохо поддается количественной оценке и/или выявлению из-за того, что зачастую он является производным, обусловленным другими рисками и уязвимыми местами системы. Ущерб репутации системы возможен в силу непредвиденных операционных проблем или из-за предоставления ошибочной или недостаточной информации конечным пользователям. Реализация репутационного риска обычно обусловлена уязвимостью других подверженных рискам областей, однако после своей реализации репутационный риск становится значимым сам по себе и требует принятия особых мер. Например, в случае распространения информации о наличии серьезных проблем у какого-либо банка возникает отдельная проблема массового изъятия вкладчиками средств из этого банка.

Риск общего управления обычно вызван отсутствием выбора стратегических мер и политики для адекватного руководства и управления системой. Риск общего управления обычно возникает в отсутствие четкого распределения ролей и ответственности и единого мнения всех участников относительно решений, касающихся целей и результатов. Риск общего управления часто обусловливает другие риски (операционный, правовой и др.), поскольку он связан с ключевыми функциями управления любой системы прямого дебета. Основные последствия данного риска — возможный конфликт интересов участников и неспособность или нежелание системы поддерживать динамику развития и инновации на рынке, а также должным образом реагировать на кризисные ситуации. Данный риск может также влиять на конкурентоспособность, если условия доступа к системам непрозрачны и не соответствуют предъявляемым к ним требованиям. Отсутствие надлежащего распределения ролей и ответственности при возникновении кризиса мешает принять своевременные меры.

4. Область применения методики наблюдения

Евросистема распространяет данную методику на систему прямого дебета SEPA. Каждый национальный центральный банк, если сочтет приемлемым, может применять эти стандарты для наблюдения и за другими платежными инструментами, не используемыми в SEPA. Поскольку цель инициативы SEPA — переход к общим стандартам, то введение наблюдения за национальными платежными системами прямого дебета должно предусматриваться, только если имеется достаточно доказательств того, что национальные системы не будут свернуты в период конечного срока создания SEPA.

Как говорится в документе “Унифицированный подход и стандарты наблюдения за платежными инструментами”, Евросистема намерена избегать дублирования в применении стандартов наблюдения за платежными инструментами и осуществлении другой деятельности по наблюдению или регулированию, например, наблюдения за системами перевода для крупных сумм или деятельности, осуществляемой в рамках банковского надзора. Поскольку в системе прямого дебета задействованы платежные системы, находящиеся под наблюдением ЕЦБ (например, для клиринга и расчета), орган управления может учитывать это при оценке рисков. Орган, осуществляющий наблюдение, может также учитывать результаты проводимого Евросистемой наблюдения и соответствующие оценки или действия органов надзора. В случае необходимости он может распространить постоянный мониторинг соответствующей банковской деятельности на участников системы прямого дебета. Данные положения, однако, не аннулируют национальные правовые обязательства или поручения, которые национальный центральный банк может иметь для платежных инструментов в рамках национальной юрисдикции.

5. Пользователи стандартов

В области наблюдения за платежными инструментами основным пользователем стандартов Евросистема рассматривает орган управления системой. Он несет ответственность за функционирование системы прямого дебета в целом, продвижение платежного инструмента и обеспечение соблюдения правил всеми участниками системы. По соглашению с органом наблюдения орган управления может назначать других участников ответственными за некоторые функции системы прямого дебета. В этих случаях следует четко разграничить ответственность данных участников (процедура должна быть прозрачна и документально оформлена). Участники должны соблюдать соответствующие стандарты (или их отдельные части) данной методики наблюдения. Наблюдение будет осуществляться с учетом распределения ответственности. Тем не менее все меры и действия, предпринимаемые в рамках системы, должны соответствовать условиям безопасности, определяемым органом управления.

Евросистема сосредоточивает свой подход к наблюдению за платежными инструментами на вопросах общесистемной значимости и контролирует орган управления системой, предлагающей платежный инструмент. Несмотря на то что такой подход является общим для Евросистемы, национальные центральные банки могут пойти дальше и задействовать иной подход и распространить его и на других участников системы, если этого потребует национальное законодательство.

6. Пять общих стандартов

С учетом вышесказанного были определены пять стандартов, регламентирующих правовые вопросы, прозрачность, операционную надежность, квалифицированное управление и устойчивые процессы клиринга и расчета. Система прямого дебета должна:

1) располагать надежной правовой базой во всех соответствующих юрисдикциях;
2) предоставлять участникам полную информацию о своей деятельности, включая сведения о финансовых рисках;
3) обладать достаточным уровнем безопасности, операционной надежности и непрерывности бизнеса;
4) иметь эффективные, контролируемые и прозрачные механизмы системы управления;
5) управлять финансовыми рисками, возникающими в процессе клиринга и расчета.

По вопросам общесистемной значимости Евросистема будет оценивать систему прямого дебета SEPA на основании данных стандартов. Для этого в соответствии с унифицированным подходом к наблюдению за платежными инструментами Евросистема намерена разработать *методологию оценки,* призванную стать руководством для всесторонней и эффективной оценки. С учетом своих правовых мандатов национальные центральные банки могут при необходимости корректировать подходы к применению методологии оценки.

Стандарт 1. Система прямого дебета должна располагать надежной правовой базой во всех соответствующих юрисдикциях

Ключевые вопросы

1.1. Правовая основа, регламентирующая создание и функционирование системы прямого дебета, взаимоотношения между органом управления и провайдером получателя платежа, провайдером плательщика, получателем платежа, плательщиком и провайдерами услуг, а также регулирующие систему правила и договорные механизмы должны быть полными, однозначными, современными, осуществимыми и соответствовать действующему законодательству.

1.2. Если данная система функционирует в разных юрисдикциях, следует проанализировать законодательство этих юрисдикций для выявления существующих противоречий. При наличии противоречий необходимо принять соответствующие меры для смягчения их последствий.

Пояснительная записка

- Отсутствие надлежащей правовой регистрации может сделать незаконными все правила и договорные механизмы, регулирующие систему прямого дебета и ее взаимоотношения с участниками.

  Если правила и договорные механизмы (включая разрешения плательщиков и поручения получателей платежей) не соответствуют действующему законодательству, они (или их определенная часть) будут недействительны, что может привести к неопределенности. Таким образом, важно уделять должное внимание соблюдению правовых норм с самого начала. Заложенные на начальной стадии основы обеспечивают надежную работу системы в будущем.

  Не полностью проработанные правила и договорные механизмы, регулирующие платежи прямого дебета между участниками (в т.ч. провайдерами платежных услуг и клиентами), могут повлиять на других участников системы. Это должно стать предметом особого внимания. Даже если орган управления не имеет прямых договорных отношений со всеми участниками, правилами данной системы можно определить соответствующие минимальные требования к решению важных для функционирования системы договорных вопросов между участниками (например, провайдерами платежных услуг и клиентами).

  При надежной правовой основе системы прямого дебета и недвусмысленности ее правил и договорных механизмов все участники будут иметь четкое понимание своих прав и обязанностей. Это уменьшит вероятность появления непредвиденных рисков и расходов, возникающих из-за двусмысленных правовых формулировок.

  Поскольку законодательство претерпевает изменения, отсутствие постоянного мониторинга правовой среды и неоперативная корректировка правил системы и договоров могут приводить к противоречиям между правилами системы и действующим законодательством и в результате — к неопределенности функционирования системы прямого дебета. Например, в силу содержания деятельности системы ее могут тщательно проверять органы, отвечающие за конкуренцию или защиту информации. В этом случае для нее могут возникнуть серьезные последствия.

- Система прямого дебета может функционировать в международном масштабе. Это усложняет задачу обеспечения правовой определенности. Более того, в этом контексте очень важно, чтобы правила и договорные механизмы (в т.ч. разрешения) содержали точные указания на действующую юрисдикцию и применяемые законы. В противном случае при возникновении коллизий юридическая сила правил системы прямого дебета и договорные механизмы могут оспариваться.

Стандарт 2. Система прямого дебета должна предоставлять участникам полную информацию о своей деятельности, включая сведения о финансовых рисках

Ключевые вопросы

2.1. Все правила и договорные механизмы, регулирующие систему прямого дебета, должны быть надлежащим образом оформлены и обновляться по мере необходимости. Все действующие и потенциальные участники должны иметь свободный доступ к необходимой информации в объеме, разрешенном законодательством о защите данных. Конфиденциальная информация должна раскрываться на основе принципа “необходимого знания” (только тем, кому положено ее знать).

2.2. Все участники (провайдеры получателей платежей, провайдеры плательщиков, получатели платежей и плательщики) должны иметь доступ к соответствующей информации для оценки рисков, включая финансовые. Более того, другие участники (например, провайдеры плательщиков и получатели платежей) должны предоставлять плательщикам достаточную информацию. В частности, плательщики должны иметь информацию об операциях прямого дебета, которые они санкционировали, и разрешениях, которые они дали, а также получать надлежащие данные об инкассо (см. Глоссарий).

Пояснительная записка

- Четкая, полная и актуальная документация необходима для бесперебойного функционирования системы прямого дебета. В отсутствие надлежащей документации (например, договоров) о ролях и обязанностях всех участников системы или надлежащего управления коммуникациями между ними может возникнуть риск общего управления. В системах прямого дебета реализация операционного риска, в т.ч. риска мошенничества, приводит к финансовым потерям одной или более сторон. Орган управления системой прямого дебета должен постоянно и своевременно в доступной форме обеспечивать всех участников информацией о способах, которые помогут снизить уровень мошенничества.

  Необходимая документация для оценки возможных рисков, возникающих в результате участия в системе прямого дебета, должна быть доступна и для потенциальных участников. Однако раскрытие конфиденциальных сведений может угрожать безопасности или репутации системы. Подобная информация должна раскрываться только тем, кому положено ее знать. Это касается и потенциальных участников, пока не принимающих участия в работе системы.

- Если не все участники (провайдеры получателей платежей, провайдеры плательщиков, получатели платежей и плательщики) имеют доступ к необходимой информации о рисках, обусловленных участием в системе, они сталкиваются с потенциальными рисками, которые возникают в ходе клиринга и расчета, а также из-за мошенничества и/или обязательств возврата средств. Сложность системы прямого дебета не позволяет идентифицировать и оценивать риски, которым участники системы могут подвергаться.

  В системах прямого дебета плательщики особенно подвержены риску несанкционированного, неразрешенного или непредвиденного дебетования их счетов. Отсутствие необходимой информации о выданных разрешениях и инкассо (или возврате средств) может вызвать у плательщиков финансовые затруднения или убытки, обусловленные непредвиденными инкассо, включая мошенничество или другие несанкционированные операции. Получатели платежей подвергаются тем же рискам при возврате средств, если они недостаточно проинформированы о получаемых платежах и связанных с ними рисках.

Стандарт 3. Система прямого дебета должна обладать достаточным уровнем безопасности, операционной надежности и непрерывности бизнеса

Ключевые вопросы

3.1. Управление безопасностью

3.1.1. Анализ рисков, связанных с безопасностью, операционной надежностью и непрерывностью бизнеса, должен проводиться и совершенствоваться, чтобы определять приемлемый уровень риска и выбирать адекватную политику и соответствующие процедуры для предотвращения, выявления, сдерживания и исправления нарушений. Соблюдение данной официальной политики следует оценивать регулярно.

3.1.2. Руководство и сотрудники всех заинтересованных сторон должны заслуживать доверие и быть в полной мере компетентными (с точки зрения навыков, профессиональной подготовки и количества сотрудников) для принятия необходимых решений, утверждения политики безопасности и выполнения своих обязательств по отношению к системе.

3.1.3. Следует дать четкие определения операционного и кризисного управления и эффективно их реализовывать. В рамках операционного управления следует осуществлять эффективный мониторинг попыток мошенничества.

3.1.4. Политика безопасности системы должна обеспечивать конфиденциальность, целостность и достоверность данных и соблюдение секретности (где необходимо, например, для электронных разрешений) на начальной стадии и при проведении операции, во время обработки, хранения или обмена данными. Следует иметь планы необходимых действий в чрезвычайных обстоятельствах в случае утечки или разглашения конфиденциальной информации.

3.1.5. Необходимо выработать и документально оформить политику контроля физического и логического доступа в систему обработки прямых дебетов. Права доступа должны быть ограничены.

3.2. Безопасность на разных стадиях (доступа, инициации, операции)

3.2.1. Для таких участников, как получатели платежей, следует сформулировать и применять адекватные требования к безопасности доступа в систему (в т.ч. во время использования электронных разрешений и их аннулирования) и при проведении операций (включая обратные операции).

3.2.2. Необходимо эффективно и надежно обрабатывать электронные разрешения и осуществлять перевод в электронную форму разрешений, переданных на бумажных носителях.

3.2.3. Следует осуществлять адекватный мониторинг деятельности плательщиков и получателей платежей в соответствии с политикой безопасности системы для своевременного выявления мошенничества и рисков, вызванных такими действиями. Следует предусмотреть необходимые меры, которые уменьшат воздействие мошенничества.

3.2.4. Необходимо предусмотреть соответствующие меры для полного осуществления прямого дебета в любое время, даже при пиковых нагрузках.

3.2.5. Следует обеспечить достаточные основания для прозрачного и легкого разрешения конфликтов, связанных с платежными операциями участников.

3.3. Клиринг и расчет

3.3.1. Механизмы клиринга и расчета должны обеспечивать адекватный уровень безопасности, операционной надежности и доступности сервисов с учетом предельных сроков расчетов, предусмотренных системой прямого дебета.

3.4. Непрерывность бизнеса

3.4.1. Анализ бизнеса в рамках данной системы должен четко определять операции, необходимые для бесперебойного функционирования системы прямого дебета. Следует иметь эффективные и комплексные планы действий на случай возникновения любого инцидента, угрожающего системе. Необходимо регулярно проверять и оценивать адекватность и эффективность этих планов.

3.5. Аутсорсинг

3.5.1. Специфическими рисками, обусловленными аутсорсингом, следует управлять на основе надлежащим образом разработанных договоров. Положения договоров должны охватывать все вопросы, за которые участник, использующий аутсорсинг, отвечает в рамках системы.

3.5.2. Следует надлежащим образом управлять и проводить мониторинг деятельности партнеров по аутсорсингу. Участники, использующие аутсорсинг, должны представлять доказательства того, что их партнеры соблюдают стандарты, за которые участники отвечают в данной системе.

Пояснительная записка

Операционные риски, включая риски мошенничества, могут серьезно влиять на систему прямого дебета и приводить к финансовым потерям участников. Они способны также подорвать доверие пользователей к системе прямого дебета. Снижение этих рисков предполагает принятие соответствующих мер, которые обеспечат следующее:

- надлежащее управление безопасностью;
- безопасность на различных стадиях (доступа, инициации, осуществления операций);
- безопасные и надежные процессы клиринга и расчета;
- непрерывность бизнеса и
- контроль аутсорсинга.

Для снижения риска мошенничества следует адекватно защитить информацию, позволяющую переводить средства со счета путем сквозной обработки. Необходимо также разработать правила быстрого выявления несанкционированных или неподтвержденных операций.

В общей модели (см. Приложение А) предусмотрено, что орган управления напрямую отвечает не за все операции и некоторые из них могут зачастую находиться в сфере конкуренции. Однако отсутствие безопасности в одной конкретной области (например, между провайдером услуг и клиентом) может оказывать влияние на другие области и, таким образом, создавать проблемы для всей системы. Даже если орган управления не контролирует все операции непосредственно, правила системы должны обеспечивать безопасность, операционную надежность и непрерывность деятельности с помощью соответствующих требований к другим участникам (например, провайдерам услуг, получателям платежей, а также к механизмам клиринга и расчета), если они применяются и относятся к функционированию всей системы. Цель подобных требований — не навязывать конкретные решения: участники должны самостоятельно нести ответственность за выбранный ими способ реализации этих требований.

- **Надлежащее управление безопасностью**

  — Без регулярного анализа операционного риска и риска безопасности, которым подвергается система, использующая общепринятые современные методологии, невозможно определить адекватную и комплексную политику безопасности для данной системы. Отсутствие надлежащего управления рисками может привести к появлению политики безопасности, которая приемлема по затратам, но не сокращает или не устраняет риски безопасности. Управлять рисками невозможно, если система управления рисками не ориентирована на поддержку политики безопасности и не привержена ей.

  — Недостаточная квалификация или недостаточное число сотрудников для решения возникающих проблем могут препятствовать бесперебойному функционированию системы прямого дебета. Недостаточные знания руководителей в области управления рисками и безопасности информационных технологий обусловливают принятие неверных решений.

  — Инциденты, связанные с нарушением безопасности, включая случаи мошенничества, могут возникать, даже если были приняты все меры предосторожности. Следовательно, необходимо отслеживать попытки мошенничества и инциденты, связанные с нарушением безопасности. Иногда невозможно определить причину инцидентов или квалифицировать вид уязвимости системы. Это обусловлено неадекватными планами действий, разработанными для уменьшения ущерба в чрезвычайных обстоятельствах, или их отсутствием. Более того, если активы недостаточно четко и всесторонне определены и оценены, трудно выявить и оценить последствия нарушения системы безопасности. Инциденты в области безопасности также возникают из-за того, что соответствующим лицам не были переданы сигналы тревоги, вследствие чего они не смогли должным образом отреагировать на сбои системы и мошенничество.

  — В результате действий неуполномоченных лиц может возникнуть угроза конфиденциальности, неприкосновенности данных, их доступности и целостности. Адекватный уровень безопасности необходим для обеспечения конфиденциальности, целостности и достоверности данных во время инициализации, хранения данных для повторных операций, осуществления и завершения операций. Защита секретных

данных особенно важна в системе прямого дебета, поскольку незаконно полученная информация (в частности, идентификаторы сквозной обработки IBAN и BIC и данные о разрешениях на списание средств) может быть также использована для получения незаконных разрешений и осуществления несанкционированных операций. Сбои могут быть не обнаружены или выявлены с большим опозданием.

— Риски, обусловленные умышленными действиями или неумышленным некорректным поведением, могут возникать в случае несанкционированных вторжений в помещения, требующие защиты, или в случае взлома секретных прикладных программ (например, программ управления счетами, инициации инкассо или хранения конфиденциальных данных).

- **Безопасность на разных стадиях (доступ, инициация, осуществление операций)**

  — Операции прямого дебета предусматривают несколько стадий: доступ пользователя в систему, разрешение (передача и отзыв) и инкассо (операция и возврат денег). Важно, чтобы меры безопасности, определенные и реализуемые участниками, распространялись на все стадии.

  — При использовании системой прямого дебета электронных разрешений или преобразованных в электронные бумажных разрешений важно гарантировать точность данных и их соответствие реальному содержанию разрешения и предварительной информации об инкассо. В противном случае это может привести к несанкционированным инкассо.

  — Без надлежащих мер безопасности и средств мониторинга действий плательщиков и получателей платежей в режиме реального времени трудно ограничить влияние мошеннических действий. Можно применять меры по снижению рисков, например, управляя действиями получателей платежей, вводя лимиты на операции. Они должны соответствовать политике безопасности системы и участников.

  — Поскольку прямой дебет широко используется для операций, повторяющихся с определенной частотой, многие операции могут проводиться в течение нескольких определенных дней каждого месяца. Кроме финансовых проблем, связанных с концентрацией этих операций, существует проблема, обусловленная ограниченностью операционных возможностей каждого участника или провайдера в этой системе (например, он может обрабатывать или хранить лишь определенный объем данных). При достижении этого лимита могут возникнуть проблемы доступности и целостности системы в дни пиковой нагрузки.

  — Разногласия между участниками нельзя разрешить, не имея прозрачной и легкодоступной информации. При частом возникновении подобных ситуаций будет подорвано доверие к системе и снижена вероятность ее дальнейшего использования.

- **Безопасный клиринг и расчет**

  — Проблемы, возникающие в процессе клиринга и расчета, могут вызывать финансовые потери, особенно у провайдеров получателей платежей и/или самих получателей платежей. Это происходит в случае неадекватного обеспечения операционной надежности, безопасности или непрерывности бизнеса. Надлежащий уровень безопасности, операционной надежности и доступности клиринга и расчета в соответствии с уровнем риска и договорными обязательствами (например, предельными сроками расчетов) важен для обеспечения целостности всех данных, участвующих в обмене в рамках клиринга и расчета.

- **Непрерывность бизнеса**

  — Катастрофы и события, негативно воздействующие на важные процессы, могут приводить к длительным простоям. Если планы мер по обеспечению непрерывности бизнеса отсутствуют или недостаточно проработаны, могут возникать проблемы, связанные с доступностью, конфиденциальностью и целостностью системы и ведущие к финансовым потерям.

- **Контроль аутсорсинга**

  — Если определенные функции системы прямого дебета передаются сторонним организациям, то соглашения об оказываемых услугах могут быть недостаточно полными или точными и/или неадекватный мониторинг предоставляемых услуг может вызвать нарушение безопасности. Для обеспечения надлежащего управления аутсорсингом необходимы соглашения с подробным описанием услуг и системы штрафов на случай мошенничества, ошибок при обработке данных или потери доступа в систему.

  — Из-за концентрации услуг в руках ограниченного числа внешних поставщиков могут возникнуть серьезные проблемы зависимости от них и проблемы доступности этих услуг.

Стандарт 4. Система прямого дебета должна использовать эффективные, контролируемые и прозрачные механизмы системы управления

Ключевые вопросы

4.1. Должны определяться и использоваться эффективные и прозрачные правила и процессы, когда:

— принимаются решения о целях и политике бизнеса, включая политику доступа;

— оцениваются деятельность, удобство и простота использования системы прямого дебета;

— выявляются риски, существенные для функционирования системы, принимаются меры по их снижению и предоставляется информация об управлении рисками.

4.2. Следует предусмотреть эффективную систему внутреннего контроля, включающую адекватную и независимую службу аудита.

Пояснительная записка

Ненадлежащее управление может негативно сказаться на системе прямого дебета. Для предупреждения, выявления и быстрого реагирования на различные сбои в работе необходимы органы, обеспечивающие эффективные решения и процессы. Чтобы сформировать доверие к системе прямого дебета, нужна современная и комплексная политика безопасности. Эффективные процессы внутреннего контроля важны для предотвращения утраты доверия к системе. Без регулирования взаимоотношений и удовлетворения надлежащим образом информационных потребностей участников могут значительно повыситься репутационные риски.

- Участниками системы прямого дебета являются провайдеры плательщиков, провайдеры получателей платежей, плательщики и получатели платежей.

  — Адекватные и прозрачные механизмы управления необходимы для того, чтобы орган управления системой прямого дебета мог принимать решения должным образом, учитывая потребности всех заинтересованных сторон. Четкая и эффективная связь — это способ обеспечить прозрачность системы. Например, прозрачный доступ предоставляет участникам и клиентам информацию о работе системы прямого дебета и обусловленных ею рисках. Он также создает условия для поддержания системой прямого дебета динамики рынка и инноваций, регулирования конфликтов интересов, возникающих в силу большого числа участников, а также своевременного и эффективного реагирования в кризисных ситуациях. Для достижения прозрачности следует также сформулировать справедливые критерии доступа в систему и выхода из нее.

  — Для бесперебойного функционирования системы прямого дебета важна ее доступность для клиентов. Для развития управления целесообразно оценивать и прогнозировать эволюцию потоков операций, с тем чтобы обеспечивать доступность системы даже в дни пиковой нагрузки. Если орган управления системой прямого дебета не получает в явной или неявной форме информацию от клиентов о том, насколько система удовлетворяет их стандарты, то потребности и ожидания клиентов могут оказаться неудовлетворенными. Это также может явиться причиной споров между участниками и/или проблем, обусловленных плохими результатами работы. Должное внимание к этим аспектам поможет сохранить доверие клиентов к системе прямого дебета.

  — Эффективные процессы управления рисками способствуют тому, что система прямого дебета должным образом предотвращает, выявляет происходящие события и реагирует на них. Эффективное управление рисками должным образом учитывает скорость технологических изменений, меняющиеся ожидания клиентуры, распространение угроз и недостатков. Оно также дает возможность выявлять наиболее существенные риски и регулярно информировать о них орган управления системой прямого дебета.

- Эффективные процессы внутреннего контроля необходимы для предотвращения и своевременного оповещения о любых сбоях, ошибках или случаях мошенничества, приводящих к потере доверия к системе прямого дебета. Анализ внутренних процессов гарантирует быстрое выявление причин ошибок, мошенничества и несогласованности и незамедлительное принятие соответствующих мер по устранению недостатков. Проведение регулярных независимых аудиторских проверок обеспечивает дополнительную уверенность в надежности действующих механизмов.

Стандарт 5. Система прямого дебета должна управлять финансовыми рисками, возникающими в процессе клиринга и расчета

Ключевые вопросы

5.1. Система прямого дебета должна выявлять финансовые риски, обусловленные клирингом и расчетом, и определять соответствующие меры управления этими рисками.

5.2. Система прямого дебета должна обеспечивать, чтобы все выбранные провайдеры клиринга и расчета имели достаточную кредитоспособность, операционную надежность и безопасность.

5.3. Если имеются договоренности о завершении расчетов в случае, когда участник не способен выполнять свои обязательства, необходимо, чтобы его принятые в расчет обязательства не превышали его доступных ресурсов, в противном случае будет поставлена под угрозу его платежеспособность. В соответствии со Стандартом 2 система прямого дебета должна также гарантировать полную осведомленность участников об их обязательствах в рамках подобных соглашений.

Пояснительная записка

- Завершенность операций прямого дебета и финансовая стабильность самой системы могут быть нарушены, если ее орган управления не оценивает (и при необходимости не снижает) финансовые риски, связанные с клирингом и расчетом.
- Неисполнение финансовых обязательств, нарушение в системе безопасности или операционный сбой по вине оператора расчетной системы могут привести к значительным, хотя и не системным, потерям. На это следует обратить особое внимание в том случае, если участники поддерживают положительное сальдо в расчетной системе. Поэтому необходимо регулярно отслеживать кредитоспособность, а также операционную надежность и обеспечение безопасности операторов систем клиринга и расчета.
- Для сдерживания кредитного риска и риска ликвидности могут предусматриваться соглашения о завершении расчетов в случае неспособности участника выполнять свои обязательства. Это приветствуется как с целью снижения финансовых рисков, так и для повышения четкости и определенности потенциальных финансовых рисков для всех участников, особенно в многосторонних системах нетто-расчетов, где реализация рисков может заблокировать цепочку расчетов и/или вызвать непредвиденный дефицит ликвидности.

Приложение А
Обзор систем прямого дебета

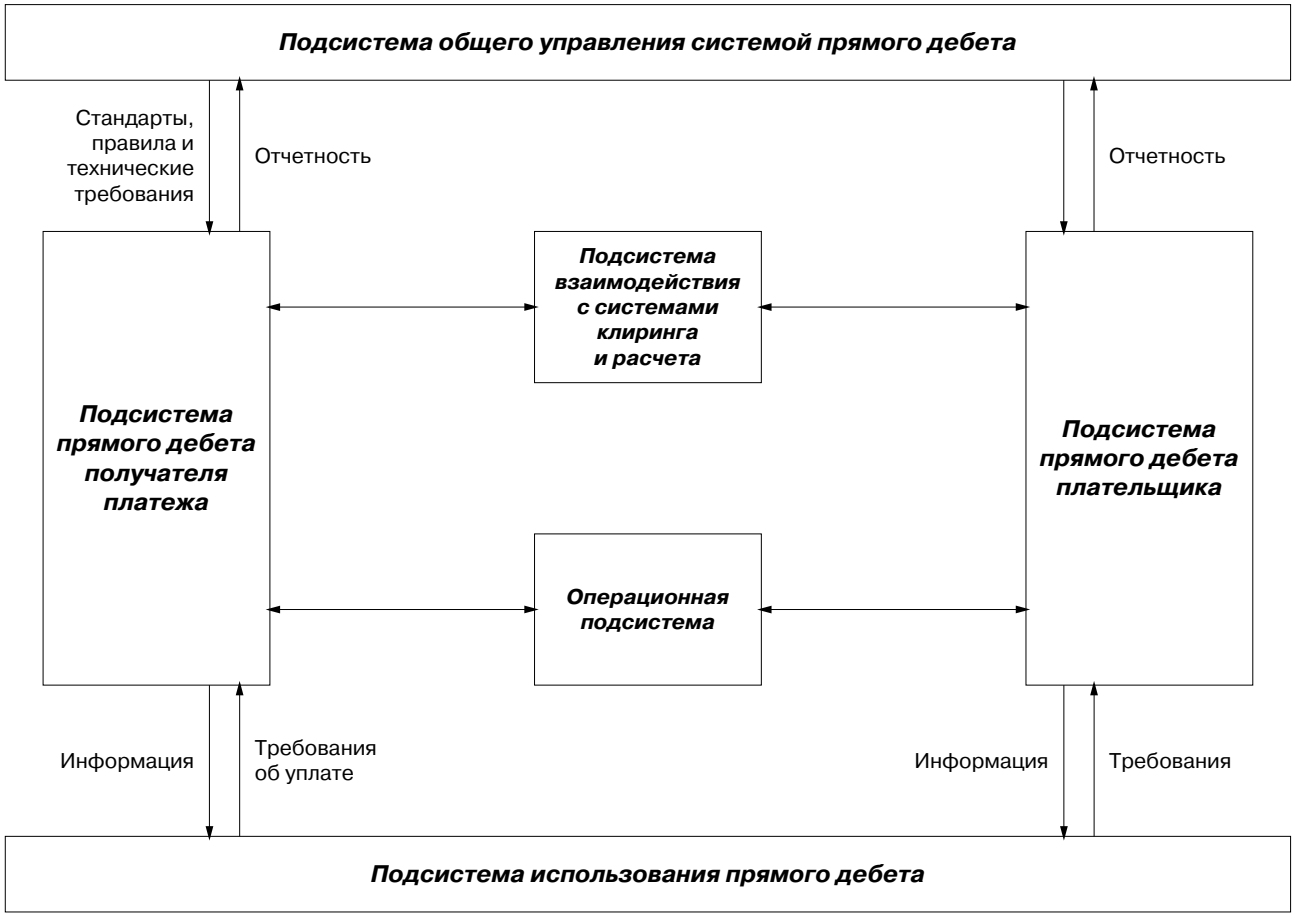
Общая модель

Система прямого дебета может быть разделена на шесть компонентов:

1) подсистема общего управления системой;
2) подсистема использования прямого дебета;
3) подсистема прямого дебета получателя платежа;
4) подсистема прямого дебета плательщика;
5) операционная подсистема;
6) подсистема взаимодействия с системами клиринга и расчета.

Различные подсистемы системы прямого дебета описаны ниже. Подсистемы представлены с учетом выполняемых задач, а не физических элементов или организаций, которые их осуществляют. Следует пояснить, что в рамках каждой подсистемы несколько организаций могут выполнять взаимосвязанные задачи.

Подсистема общего управления системой прямого дебета



Подсистема общего управления системой отвечает за управление, включая, например, определение и разработку стандартов, правил, технических требований или отбор и одобрение уже существующих, а также политик доступа в систему, конкуренции, ценообразования, предотвращения мошенничества, управления, мониторинга деятельности, соблюдения стандартов, решения спорных вопросов и т.д. Например, в системе прямого дебета SEPA большинство этих функций выполняет Европейский платежный совет (EPC) (Пленарный комитет или Подкомитет управления схемой прямого дебета).

Подсистема прямого дебета получателя платежа включает, в частности, аккредитацию и управление получателями платежей, мониторинг деятельности и случаев мошенничества, верификацию, экспедирование и исполнение операций (включая обратные операции). Эта деятельность осуществляется в основном провайдером получателя платежа.

Подсистема прямого дебета плательщика отвечает за взаимоотношения с плательщиками и выполнение операций. Эта деятельность в основном осуществляется провайдером плательщика.

Подсистема использования прямого дебета охватывает взаимоотношения между плательщиком и получателем платежа (разрешения, информацию о проводимых трансакциях по переводу средств).

Операционная подсистема предоставляет технические и организационные услуги, например, услуги телекоммуникационных сетей, позволяющих осуществлять обмен данными между провайдером получателя платежа и провайдером плательщика на разных стадиях или предоставляющих другие услуги, например, размещение идентификаторов плательщика и получателя. Эта деятельность может быть особой для системы прямого дебета или общей с другими услугами и может осуществляться теми же организациями, что выполняют клиринг и расчет.

Подсистема взаимодействия с системами клиринга и расчета затрагивает всю деятельность и инфраструктуру, необходимые для двустороннего или многостороннего клиринга и расчета по операциям прямого дебета. В рамках данной подсистемы могут использоваться разные формы клиринга и расчета.

Приложение Б
Глоссарий терминов и определений

В разных системах прямого дебета существует разная терминология. Применяемые в настоящем документе определения соответствуют, насколько это возможно, определениям, изложенным в "Директиве по платежным услугам" и применяемым Европейским платежным советом. В данном документе использовались следующие определения:

Аутсорсинг (outsourcing) — положение, когда провайдер услуг привлекает по договору третью сторону для выполнения своих обязанностей в системе прямого дебета. Каждый провайдер несет полную ответственность за осуществляемую за него деятельность по договору об аутсорсинге. Провайдер услуг должен обеспечивать, чтобы все работы по аутсорсингу управлялись и контролировались так, как если бы они выполнялись самим провайдером услуг.

Инкассо (collection) — в рамках данного документа это процесс, с помощью которого провайдеры платежных услуг переводят средства плательщика получателю платежа.

Клиенты (customers) системы прямого дебета — это стороны сделки — получатель платежа и плательщик, — пользующиеся услугами системы прямого дебета.

- **Получатель платежа (payee)** (или кредитор) — физическое или юридическое лицо — предполагаемый получатель средств.
- **Плательщик (payer)** (или дебитор) — физическое или юридическое лицо, имеющее платежный счет и санкционирующее операцию прямого дебета к своему платежному счету.

Операционная стадия (transaction phase) — процесс осуществления платежа посредством прямого дебета, начиная с инкассо, инициированного получателем платежа, до его завершения (обычное исполнение или отклонение, возврат или возмещение средств).

Платежный счет (payment account) — счет, используемый для выполнения платежных операций.

Провайдеры платежных услуг (payment service providers) — согласно PSD это: (а) кредитные организации; (б) учреждения, осуществляющие операции с электронными деньгами; (в) почтовые жироорганизации[5]; (г) платежные учреждения; (д) Европейский центральный банк и национальные центральные банки, действующие не в качестве монетарных властей или других государственных органов, и (е) государства — члены ЕС или их региональные или местные органы, действующие не в качестве государственных органов власти.

- **Провайдер платежных услуг плательщика (payer's payment service providers)** — провайдер платежных услуг, у которого открыт платежный счет, подлежащий дебетованию, и который заключил соглашение с плательщиком о правилах и условиях предоставления продукта с помощью данной системы. На основе этого соглашения он каждый раз выполняет инкассо, инициированное получателем платежа, путем дебетования счета плательщика.
- **Провайдер платежных услуг получателя платежа (payee's payment service providers)** — провайдер платежных услуг, который открыл платежный счет получателя и заключил с ним соглашение о правилах и условиях предоставления продукта с помощью данной системы. На основе этого соглашения он каждый раз получает и исполняет инструкции получателя платежа инициировать операции прямого дебета.

Прямой дебет (direct debit) — платежная услуга по списанию средств с платежного счета плательщика, при которой получатель платежа инициирует платежную сделку на основе согласия плательщика, данного получателю платежа, провайдеру получателя платежа или провайдеру плательщика.

Разрешение (mandate) — санкционирование (согласие), данное плательщиком получателю платежа и/или своему провайдеру дебетовать счет. Разрешение может быть в виде бумажного документа, подписанного плательщиком. Оно может быть электронным документом, созданным и подписанным надежным электронным способом. Разрешение на бумажном или электронном носителе должно содержать необходимый юридический текст и наименования подписавших его сторон. В некоторых национальных вариантах систем прямого дебета (например, при одноразовых сделках прямого дебета) разрешение не используется.

Система прямого дебета (direct debit scheme) — набор функций, процедур, механизмов, правил и устройств, позволяющих осуществлять санкционированное дебетование платежного счета плательщика, инициированное получателем платежа, либо отдельным платежом, либо серией платежей.

[5] Почтовые организации, оказывающие ограниченные банковские услуги, в т.ч. услуги по приему и осуществлению розничных платежей.

Стадия доступа (access phase) означает доступ участников (провайдеров или клиентов) в систему.

Стадия инициации (initiation phase) включает создание, управление и завершение (аннулирование или отзыв) разрешения.

Участниками (actors) системы прямого дебета являются орган управления, провайдер плательщика, провайдер получателя платежа, провайдеры услуг (в частности, для операционной подсистемы и подсистемы клиринга и расчета), клиенты (получатель платежа и плательщик).

R — операции, или обратные операции (R-transactions) — общий термин для следующих понятий:

- **Возмещение —** требования плательщика о возмещении средств с оспариваемого дебетованного счета.
- **Отказы —** инструкции, выданные по каким-либо причинам плательщиком до осуществления расчета, с тем чтобы провайдер плательщика не осуществлял платеж в виде прямого дебета.
- **Отклонение —** результат неисполненной операции, при которой платеж отклонен до проведения межбанковского расчета. К возможным причинам относятся технические сбои, закрытие счета, недостаток средств.
- **Возвраты —** инкассо прямого дебета, отличающиеся от обычного исполнения, следующие за межбанковскими расчетами и инициированные провайдером плательщика.
- **Аннулирование** инициируется получателем платежа после расчета в случае проведения оплаты, которая не должна была состояться. Следовательно, это — возмещение средств получателем платежа плательщику.
- **Отзыв —** требование получателя платежа вернуть средства до того, как их получит провайдер получателя платежа.

НАБЛЮДЕНИЕ ЗА СИСТЕМАМИ КРЕДИТОВЫХ ПЕРЕВОДОВ. СТАНДАРТЫ

Европейский центральный банк

Август 2009 г.

Содержание

1. Введение*

У центральных банков есть четко поставленная цель — укрепление финансовой стабильности и обеспечение надежности платежных и расчетных систем. Согласно Статье 105 (2) "Соглашения об учреждении Европейского сообщества" и Статьям 3 и 22 "Устава Европейской системы центральных банков и Европейского центрального банка" одна из основных задач Евросистемы заключается в "обеспечении бесперебойной работы платежных систем".

В феврале 2009 года Евросистема приняла решение дать более точное определение своей функции наблюдения и опубликовала новый документ о политике осуществления наблюдения[1]. В нем приводится общее представление о наборе механизмов и инструментов, применяемых Евросистемой, и подчеркивается, что платежные инструменты являются важным элементом платежных систем. Риски, связанные с предоставлением и использованием платежных инструментов в основном не рассматривались как системные, но безопасность и эффективность платежных инструментов необходимы, чтобы поддерживать доверие к денежному обращению и обеспечивать эффективность экономики.

Создание Единого пространства платежей в евро (SEPA) существенно меняет ситуацию с розничными платежами и повышает значимость согласованного подхода к наблюдению за платежными инструментами. Вследствие этого Евросистема разработала обобщенный подход и минимальный набор общих стандартов наблюдения за платежными инструментами, которые описаны в документе "Унифицированный подход и стандарты наблюдения за платежными инструментами" (ЕЦБ, февраль 2009 года). Цель этих стандартов — создать универсальную основу для наблюдения за всеми платежными инструментами, достаточно гибко подходя к особенностям отдельных инструментов. Данные стандарты закладывают фундамент для развития наблюдения за схемами прямого дебета и кредитовыми переводами в SEPA, а также для новых платежных инструментов, используемых в SEPA. Более того, каждый национальный центральный банк может также при необходимости применять общие стандарты при осуществлении наблюдения за другими национальными (не используемыми в SEPA) платежными инструментами. Чтобы учесть специфику каждого платежного инструмента, к которому применяются общие стандарты наблюдения, содержание каждого шага, предусмотренного унифицированным подходом Евросистемы к наблюдению за платежными инструментами, необходимо по-разному адаптировать для учета особенностей анализируемого платежного инструмента.

Настоящий документ описывает, как общие стандарты должны быть адаптированы к специфическим особенностям систем кредитовых переводов. В нем система кредитовых переводов определяется как набор функций, процедур, механизмов, правил и инструментов в бумажном или электронном виде, позволяющих исполнять платежные распоряжения, направленные плательщиком своему провайдеру платежных услуг (PSP)[2] с целью перевода средств под управление получателя. Плательщик (или инициатор) является физическим или юридическим лицом, которое дает платежное распоряжение; получатель средств (или бенефициар) является физическим или юридическим лицом — целевым получателем денежных средств, предмета платежной операции. Перевод денежных средств осуществляется посредством дебетования и кредитования счетов независимо от способа, с помощью которого плательщик предоставляет эти средства (плательщик может открыть счет или предоставлять средства в наличной форме). Другие термины, используемые в данном документе, разъясняются в "Глоссарии терминов и определений" (Приложение Б).

Методика наблюдения базируется на использовании принципа декомпозиции и риск-ориентированного подхода, учитывающего, в частности, условия функционирования рынка кредитовых переводов и управляющего соответствующими рисками, которым подвержены системы кредитовых переводов на протяжении всего платежного цикла, включая клиринг и расчет.

Методика наблюдения затрагивает весь цикл платежа, включая стадии доступа к системе кредитового перевода, операционную стадию, клиринг и расчет. Она учитывает особенности системы розничных платежей и используемого платежного инструмента.

Цель наблюдения за системами кредитовых переводов — обеспечить надежность и эффективность платежей с помощью этих инструментов. Системы кредитовых переводов могут быть подвержены различным рискам, как любая платежная система. Они должны быть защищены от всех рисков, которые способны оказать всеобъемлющее влияние на доверие пользователей к данному инструменту. Следует четко разграничить проблемы системного характера (например, нарушение общепринятых правил или стандартов безопасности, которое

---

* Данный материал является неофициальным переводом публикации ЕЦБ "Oversight framework for credit transfer schemes" ("Наблюдение за системами кредитовых переводов. Стандарты"). Электронная версия данной публикации на английском языке размещена на веб-сайте ЕЦБ *(http://www.ecb.int/pub/pdf/other/oversightframeworkcredittransferschemesen.pdf)*.

[1] ЕЦБ, "Основы политики наблюдения Евросистемы", 2009 год.

[2] Определение дано в заголовке 1 Статьи 4 (9) "Директивы 2007/64/ЕС Европейского парламента и Совета ЕС" от 13 ноября 2007 года о платежных услугах на внутреннем рынке.

подвергнет риску всех или большинство участников) и проблемы отдельных участников (например, неплатежеспособность одного из них, которая преодолевается в рамках банковского надзора) или проблемы, остроту которых надлежит смягчить отдельному участнику. Кроме того, особенно важно создать эффективные механизмы управления, а также помнить о необходимости предотвратить любой ущерб, угрожающий репутации используемого инструмента.

Данный документ построен следующим образом: Раздел 2 характеризует структуру стандартов по наблюдению; Раздел 3 обобщает различные риски, которым подвергаются участники системы кредитовых переводов; Раздел 4 дает представление об области применения методики; в Разделе 5 определены пользователи стандартов; в Разделе 6 описаны сами стандарты. В Приложениях представлены обзор систем кредитовых переводов и глоссарий терминов.

2. Структура стандартов

Методика наблюдения следует "Унифицированному подходу и стандартам наблюдения за платежными инструментами" Евросистемы[3]. Общепринятые стандарты были разработаны на основе выявленных типов рисков (см. Раздел 3). Методика учитывает специфику систем кредитовых переводов, в частности, обусловленную особенностями операционной деятельности и обеспечения безопасности.

Каждый общепринятый стандарт наблюдения содержит ряд ключевых вопросов, которые рассмотрены и разъяснены в пояснительных записках.

3. Типы рисков

Участники системы могут подвергаться определенным рискам. Платеж может быть не исполнен по различным причинам (обсуждаемым далее), например, из-за мошенничества, операционных сбоев или финансового положения одного из участников. Для систем кредитовых переводов выявлены различные риски, в частности, правовой, операционный, репутационный или связанный с общим управлением.

Правовой риск относится к риску убытков, которые возникли в результате неожиданного применения закона или правовой нормы или невозможности добиться исполнения договора. Правовой риск возникает в связи с правовой неопределенностью в области реализации прав и обязанностей сторон, вовлеченных в систему кредитовых переводов. В системе кредитовых переводов правовой риск может влиять на различные стадии и затрагивать разных участников системы. Правовая структура международной системы кредитовых переводов является еще более сложной, поскольку должна учитывать требования различных регулирующих систем для обеспечения ее правомочности в условиях соответствующих юрисдикций.

Финансовый риск охватывает ряд возникающих при финансовых сделках рисков, включая риск ликвидности и кредитный риск. Стандарты наблюдения призваны понизить уровень финансовых рисков, в т.ч. потенциальные убытки, обусловленные операционным риском (например, риском мошенничества). В рамках системы кредитовых переводов финансовые риски могут возникать у всех участников, получателей платежей, плательщиков и провайдеров платежных услуг. На стадии клиринга и расчета в системе кредитовых переводов финансовые риски могут быть вызваны дефолтом или неплатежеспособностью расчетного агента или провайдеров услуг.

Операционный риск возникает в результате неадекватных или давших сбой внутренних процессов или систем, ошибок персонала, эксплуатирующего систему, или внешних событий, повлиявших на любой элемент системы кредитовых переводов. Операционный риск может быть вызван неспособностью исполнить или завершить одну или несколько стадий платежного процесса. Операционный риск часто связан с доступностью системы кредитовых переводов.

Операционный риск включает риск мошенничества, определяемый как злонамеренный, или преступный, обман, который может привести к финансовым потерям одной из сторон, вовлеченных в сделку, и который, возможно, отражает неадекватные механизмы безопасности. Основной риск мошенничества представляет собой несанкционированное списание средств со счета плательщика. Возникновение некоторых рисков мошенничества обусловлено определенными технологическими решениями, например, спецификой маршрутизации и проверки распоряжений. Поскольку кредитовые переводы в основном используются при межбанковских переводах, важна борьба с внутренним мошенничеством.

[3] ЕЦБ, "Унифицированный подход и стандарты наблюдения за платежными инструментами", 2009 год.

Репутационный риск можно определить как вероятность обоснованного или необоснованного ухудшения репутации системы, которое приводит к сокращению клиентской базы, затратным судебным процессам, снижению доходов, проблемам с ликвидностью или значительному уменьшению рыночной капитализации. Сложность системы кредитовых переводов и высокий уровень автоматизации операционных процессов затрудняют понимание клиентами нюансов ее работы. Однако системы кредитовых переводов, как правило, тесно связаны с автоматизированными системами конечных бизнес-пользователей, которые способны оценить, насколько определенная система кредитовых переводов может удовлетворить их операционные потребности. Это наряду с репутацией и стоимостью услуг является для конечных пользователей важным параметром при выборе системы. Репутационный риск плохо поддается количественной оценке и/или выявлению из-за того, что зачастую он является производным, обусловленным другими рисками и уязвимыми местами системы. Ущерб репутации системы возможен в силу непредвиденных операционных проблем или из-за предоставления ошибочной или недостаточной информации конечным пользователям. Реализация репутационного риска обычно обусловлена уязвимостью других подверженных рискам областей, однако после своей реализации репутационный риск становится значимым сам по себе и требует принятия особых мер. Например, в случае распространения информации о наличии серьезных проблем у какого-либо банка возникает отдельная проблема массового изъятия вкладчиками средств из этого банка.

Риск общего управления обычно вызван отсутствием выбора стратегических мер и политики для адекватного руководства и управления системой. Риск общего управления обычно возникает в отсутствие четкого распределения ролей и ответственности и единого мнения всех участников относительно решений, касающихся целей и результатов. Риск общего управления часто обусловливает другие риски (операционный, правовой и др.), поскольку он связан с ключевыми функциями управления любой системы кредитовых переводов. Основные последствия данного риска — возможный конфликт интересов участников и неспособность или нежелание системы поддерживать динамику развития и инновации на рынке, а также должным образом реагировать на кризисные ситуации. Данный риск может также влиять на конкурентоспособность, если условия доступа к системам непрозрачны и не соответствуют предъявляемым к ним требованиям. Отсутствие надлежащего распределения ролей и ответственности при возникновении кризиса мешает принять своевременные меры.

4. Область применения методики наблюдения

Евросистема распространяет данную методику на систему кредитовых переводов SEPA. Каждый национальный центральный банк, если сочтет приемлемым, может применять эти стандарты для наблюдения и за другими платежными инструментами, не используемыми в SEPA. Поскольку цель инициативы SEPA — переход к общим стандартам, то введение наблюдения за национальными платежными системами кредитовых переводов должно предусматриваться, только если имеется достаточно доказательств того, что национальные системы не будут свернуты в период конечного срока создания SEPA.

Как говорится в документе “Унифицированный подход и стандарты наблюдения за платежными инструментами”, Евросистема намерена избегать дублирования в применении стандартов наблюдения за платежными инструментами и осуществлении другой деятельности по наблюдению или регулированию, например, наблюдения за системами платежей для крупных сумм или деятельности, осуществляемой в рамках банковского надзора. Поскольку в системе кредитовых переводов задействованы платежные системы, находящиеся под наблюдением ЕЦБ (например, для клиринга и расчета), орган управления может учитывать это при оценке рисков. Орган, осуществляющий наблюдение, может также учитывать результаты проводимого Евросистемой наблюдения и соответствующие оценки или действия органов надзора. Он в случае необходимости может распространить постоянный мониторинг соответствующей банковской деятельности на участников системы кредитовых переводов. Данные положения, однако, не аннулируют национальные правовые обязательства или поручения, которые национальный центральный банк может иметь для платежных инструментов в рамках национальной юрисдикции.

5. Пользователи стандартов

В области наблюдения за платежными инструментами Евросистема *основным пользователем стандартов рассматривает орган управления системой.* Он несет ответственность за функционирование системы кредитовых переводов в целом, продвижение платежного инструмента и обеспечение соблюдения правил всеми участниками системы. По соглашению с органом наблюдения орган управления может назначать других участников ответственными за некоторые функции системы кредитовых переводов. В этих случаях следует четко разграничить ответственность данных участников (процедура должна быть прозрачна и документально оформлена).

Участники должны соблюдать соответствующие стандарты (или их отдельные части) настоящей методики наблюдения. Наблюдение будет осуществляться с учетом распределения ответственности. Тем не менее все меры и действия, предпринимаемые в рамках системы, должны соответствовать условиям безопасности, определяемым органом управления.

Евросистема сосредоточивает свой подход к наблюдению за платежными инструментами на вопросах общесистемной значимости и контролирует орган управления системой, предлагающей платежный инструмент. Несмотря на то что такой подход является общим для Евросистемы, национальные центральные банки могут пойти дальше и задействовать иной подход и распространить его и на других участников системы, если этого потребует национальное законодательство.

6. Пять общих стандартов

С учетом вышесказанного были определены пять стандартов, регламентирующих правовые вопросы, прозрачность, операционную надежность, квалифицированное управление и устойчивые процессы клиринга и расчета. Система кредитовых переводов должна:

1) располагать надежной правовой базой во всех соответствующих юрисдикциях;
2) предоставлять участникам полную информацию о своей деятельности, включая сведения о финансовых рисках;
3) обладать достаточным уровнем безопасности, операционной надежности и непрерывности бизнеса;
4) иметь эффективные, контролируемые и прозрачные механизмы системы управления;
5) управлять финансовыми рисками, возникающими в процессе клиринга и расчета.

По вопросам общесистемной значимости система кредитовых переводов SEPA будет оцениваться Евросистемой на основании данных стандартов. Для этого в соответствии с унифицированным подходом к наблюдению за платежными инструментами Евросистема намерена разработать *методологию оценки,* призванную стать руководством для всесторонней и эффективной оценки. С учетом своих правовых мандатов национальные центральные банки могут при необходимости корректировать свои подходы к применению методологии оценки.

Стандарт 1. Система кредитовых переводов должна располагать надежной правовой базой во всех соответствующих юрисдикциях

Ключевые вопросы

1.1. Правовая основа, регламентирующая создание и функционирование системы кредитовых переводов, взаимоотношения между органом управления и провайдером получателя платежа, провайдером плательщика, получателем платежа, плательщиком и провайдерами услуг[4], а также регулирующие систему правила и договорные механизмы должны быть полными, однозначными, современными, осуществимыми и соответствовать действующему законодательству.

1.2. Если данная система функционирует в разных юрисдикциях, следует проанализировать законодательство этих юрисдикций для выявления существующих противоречий. При наличии противоречий необходимо принять соответствующие меры для смягчения их последствий.

Пояснительная записка

- Отсутствие надлежащей правовой регистрации может сделать незаконными все правила и договорные механизмы, регулирующие систему кредитовых переводов и ее взаимоотношения с участниками.

  Если правила и договорные механизмы не соответствуют действующему законодательству, они (или их определенная часть) будут недействительны, что может привести к неопределенности. Таким образом, важно уделять должное внимание соблюдению правовых норм с самого начала. Заложенные на начальной стадии основы обеспечивают надежную работу системы в будущем.

  Не полностью проработанные правила и договорные механизмы, регулирующие кредитовые переводы между участниками (в т.ч. провайдерами платежных услуг и клиентами), могут повлиять на других участников системы. Это должно стать предметом особого внимания. Даже если орган управления не имеет прямых договорных отношений со всеми участниками, правилами данной системы можно определить соответствующие минимальные требования к решению важных для функционирования системы договорных вопросов между участниками (например, провайдерами платежных услуг и клиентами).

  При надежной правовой основе системы кредитовых переводов и недвусмысленности ее правил и договорных механизмов все участники будут иметь четкое понимание своих прав и обязанностей. Это уменьшит вероятность появления непредвиденных рисков и расходов, возникающих из-за двусмысленных правовых формулировок.

  Поскольку законодательство претерпевает изменения, отсутствие постоянного мониторинга правовой среды и неоперативная корректировка правил системы и договоров могут приводить к противоречиям между правилами системы и действующим законодательством и в результате — к неопределенности функционирования системы кредитовых переводов. Например, в силу содержания деятельности системы ее могут тщательно проверять органы, отвечающие за конкуренцию или защиту информации. В этом случае для нее могут возникнуть серьезные последствия.

- Система кредитовых переводов может функционировать в международном масштабе. Это усложняет задачу обеспечения правовой определенности. Более того, в этом контексте очень важно, чтобы правила и договорные механизмы (в т.ч. разрешения) содержали четкое указание на действующую юрисдикцию и применяемые законы. В противном случае при возникновении коллизий юридическая сила правил системы кредитовых переводов и договорные механизмы могут оспариваться.

[4] Провайдеры услуг информационно-телекоммуникационных систем, провайдеры систем клиринга и расчета.

Стандарт 2. Система кредитовых переводов должна предоставлять участникам полную информацию о своей деятельности, включая сведения о финансовых рисках

Ключевые вопросы

2.1. Все правила и договорные механизмы, регулирующие систему кредитовых переводов, должны быть надлежащим образом оформлены и обновляться по мере необходимости. Все действующие и потенциальные участники должны иметь свободный доступ к необходимой информации в объеме, разрешенном законодательством о защите данных. Конфиденциальная информация должна раскрываться на основе принципа “необходимого знания” (только тем, кому положено ее знать).

2.2. Все участники (провайдеры получателей платежей, провайдеры плательщиков, получатели платежей и плательщики) должны иметь доступ к соответствующей информации для оценки рисков, включая финансовые.

Пояснительная записка

- Четкая, полная и актуальная документация необходима для бесперебойного функционирования системы кредитовых переводов. В отсутствие надлежащей документации (например, договоров) о ролях и обязанностях всех участников системы или надлежащего управления коммуникациями между ними может возникнуть риск общего управления. В системах кредитовых переводов реализация операционного риска, в т.ч. риска мошенничества, приводит к финансовым потерям одной или более сторон. Орган управления системой кредитовых переводов должен постоянно и своевременно в доступной форме обеспечивать всех участников информацией о способах, которые помогут снизить уровень мошенничества.

  Необходимая документация для оценки возможных рисков, возникающих в результате участия в системе кредитовых переводов, должна быть доступна и для потенциальных участников. Однако раскрытие конфиденциальных сведений может угрожать безопасности или репутации системы. Подобная информация должна раскрываться только тем, кому положено ее знать. Это касается и потенциальных участников, пока не принимающих участия в работе системы.

- Если не все участники (провайдеры получателей платежей, провайдеры плательщиков, получатели платежей и плательщики) имеют доступ к необходимой информации о рисках, обусловленных участием в системе, они сталкиваются с потенциальными рисками, которые возникают в ходе клиринга и расчета, а также из-за мошенничества и/или обязательств возврата средств. Сложность системы кредитовых переводов не позволяет идентифицировать и оценивать риски, которым участники системы могут подвергаться.

  В системах кредитовых переводов плательщики подвержены риску несанкционированного, неразрешенного или непредвиденного дебетования их счетов. Отсутствие необходимой информации о технологических решениях и операционных процедурах (таких, как маршрутизация и проверка распоряжений) может вызвать у плательщиков финансовые затруднения или убытки, обусловленные непредвиденными платежными распоряжениями, включая мошенничество или другие несанкционированные операции.

Стандарт 3. Система кредитовых переводов должна обладать достаточным уровнем безопасности, операционной надежности и непрерывности бизнеса

Ключевые вопросы

3.1. Управление безопасностью

3.1.1. Анализ рисков, связанных с безопасностью, операционной надежностью и непрерывностью бизнеса, должен проводиться и совершенствоваться, чтобы определять приемлемый уровень риска и выбирать адекватную политику и соответствующие процедуры для предотвращения, выявления, сдерживания и исправления нарушений. Соблюдение данной официальной политики следует оценивать регулярно.

3.1.2. Руководство и сотрудники всех заинтересованных сторон должны заслуживать доверие и быть в полной мере компетентными (с точки зрения навыков, профессиональной подготовки и количества сотрудников) для принятия необходимых решений, утверждения политики безопасности и выполнения своих обязательств по отношению к системе.

3.1.3. Следует дать четкие определения операционного и кризисного управления и эффективно их реализовывать. В рамках операционного управления следует осуществлять эффективный мониторинг попыток мошенничества.

3.1.4. Политика безопасности системы должна обеспечивать конфиденциальность, целостность и достоверность данных и соблюдение секретности (где необходимо, например, при операциях доступа в системы дистанционного банковского обслуживания, аутентификации плательщика и проверки распоряжений) на всех стадиях, во время обработки, хранения или обмена данными. Следует иметь планы необходимых действий в чрезвычайных обстоятельствах в случае утечки или разглашения конфиденциальной информации.

3.1.5. Необходимо выработать и документально оформить политику контроля физического и логического доступа в систему обработки кредитовых переводов. Права доступа должны быть ограничены.

3.2. Безопасность на разных стадиях (доступа, операции)

3.2.1. Следует сформулировать и применять адекватные требования к безопасности на стадии доступа в систему (в т.ч. определение процедур безопасности при обработке платежных распоряжений, переданных через системы дистанционного банковского обслуживания, включая доставку аппаратных средств или кодов/паролей для аутентификации участника системы) и на операционной стадии (включая обратные операции).

3.2.2. Эффективные и безопасные процедуры должны:

(i) использоваться при передаче платежного распоряжения (в бумажной или электронной форме) от плательщика к провайдеру платежных услуг;

(ii) применяться при аутентификации платежных распоряжений, а также для исключения возможности несанкционированного списания средств со счета плательщика, открытого у провайдера платежных услуг.

3.2.3. Следует осуществлять адекватный мониторинг деятельности плательщиков и получателей платежей в соответствии с политикой безопасности системы для своевременного выявления мошенничества и рисков, вызванных такими действиями. Следует предусмотреть необходимые меры, которые уменьшат воздействие мошенничества.

3.2.4. Необходимо предусмотреть соответствующие меры для полного осуществления кредитовых переводов в любое время, даже при пиковых нагрузках.

3.2.5. Следует обеспечить достаточные основания для прозрачного и легкого разрешения конфликтов, связанных с платежными операциями участников.

3.3. Клиринг и расчет

3.3.1. Механизмы клиринга и расчета должны обеспечивать адекватный уровень безопасности, операционной надежности и доступности сервисов с учетом предельных сроков расчетов, предусмотренных системой кредитовых переводов.

3.4. Непрерывность бизнеса

3.4.1. Анализ бизнеса в рамках данной системы должен четко определять операции, необходимые для бесперебойного функционирования системы кредитовых переводов. Следует иметь эффективные и комплексные планы действий на случай возникновения любого инцидента, угрожающего системе. Необходимо регулярно проверять и оценивать адекватность и эффективность этих планов.

3.5. Аутсорсинг

3.5.1. Специфическими рисками, обусловленными аутсорсингом, следует управлять на основе надлежащим образом разработанных договоров. Положения договоров должны охватывать все вопросы, за которые участник, использующий аутсорсинг, отвечает в рамках системы.

3.5.2. Следует надлежащим образом управлять и проводить мониторинг деятельности партнеров по аутсорсингу. Участники, использующие аутсорсинг, должны представлять доказательства того, что их партнеры соблюдают стандарты, за которые участники отвечают в данной системе.

Пояснительная записка

Операционные риски, включая риски мошенничества, могут серьезно влиять на систему кредитовых переводов и приводить к финансовым потерям участников. Они способны также подорвать доверие пользователей к системе кредитовых переводов. Снижение этих рисков предполагает принятие соответствующих мер, которые обеспечат следующее:

- надлежащее управление безопасностью;
- безопасность на различных стадиях (доступа, операции);
- безопасные и надежные процессы клиринга и расчета;
- непрерывность бизнеса и
- контроль аутсорсинга.

Для снижения риска мошенничества следует адекватно защитить информацию, позволяющую переводить средства со счета путем сквозной автоматизированной обработки. Необходимо также разработать правила быстрого выявления несанкционированных или неподтвержденных операций.

В общей модели (см. Приложение А) предусмотрено, что орган управления напрямую отвечает не за все операции, и некоторые из них могут зачастую находиться в сфере конкуренции. Однако отсутствие безопасности в одной конкретной области (например, между провайдером услуг и клиентом) может оказывать влияние на другие области и, таким образом, создавать проблемы для всей системы. Даже если орган управления не контролирует все операции непосредственно, правила системы должны обеспечивать безопасность, операционную надежность и непрерывность бизнеса с помощью соответствующих требований к другим участникам (например, провайдерам услуг, получателям платежей, а также к механизмам клиринга и расчета), если они применяются и относятся к функционированию всей системы. Цель подобных требований не должна заключаться в навязывании конкретных решений: участники должны самостоятельно нести ответственность за выбранный ими способ реализации этих требований.

- **Надлежащее управление безопасностью**

  — Без регулярного анализа операционного риска и риска безопасности, которым подвергается система, использующая общепринятые современные методологии, невозможно определить адекватную и комплексную политику безопасности для данной системы. Отсутствие надлежащего управления рисками может привести к появлению политики безопасности, которая приемлема по затратам, но не сокращает или не устраняет риски безопасности. Управлять рисками невозможно, если система управления рисками не ориентирована на поддержку политики безопасности и не привержена ей.

  — Недостаточная квалификация или недостаточное число сотрудников для решения возникающих проблем могут препятствовать бесперебойному функционированию системы кредитовых переводов. Недостаточные знания руководителей в области управления рисками и безопасности информационных технологий обусловливают принятие неверных решений.

  — Инциденты, связанные с нарушением безопасности, включая случаи мошенничества, могут возникать, даже если были приняты все меры предосторожности. Следовательно, необходимо отслеживать попытки мошенничества и инциденты, связанные с нарушением безопасности. Иногда невозможно определить причину инцидента или квалифицировать вид уязвимости системы. Это обусловлено неадекватными планами действий, разработанными для уменьшения ущерба в чрезвычайных обстоятельствах, или их отсутствием. Более того, если активы недостаточно четко и всесторонне определены и оценены, трудно выявить и оценить последствия нарушения системы безопасности. Инциденты в области безопасности

также возникают из-за того, что соответствующим лицам не были переданы сигналы тревоги, вследствие чего они не смогли должным образом отреагировать на сбои системы и мошенничество.

— В результате действий неуполномоченных лиц может возникнуть угроза конфиденциальности, неприкосновенности данных, их доступности и целостности. Адекватный уровень безопасности необходим для обеспечения конфиденциальности, целостности и достоверности данных во время осуществления платежа (с момента создания платежного распоряжения) и хранения данных для повторных операций. Способы обеспечения безопасности (такие, как коды/пароли и аппаратные устройства аутентификации), используемые при доступе к системам дистанционного банковского обслуживания, аутентификации плательщика и проверке платежного распоряжения, могут быть раскрыты или скомпрометированы, если не применяются надлежащие процедуры управления безопасностью. Защита данных важна в системе кредитовых переводов, поскольку незаконно полученная информация (в частности, идентификаторы сквозной обработки IBAN и BIC и данные о разрешениях на списание средств) может быть использована для осуществления несанкционированных операций в системе кредитовых переводов или других платежных системах (например, получения незаконных разрешений в системе прямого дебета). Связанные с этим риски могут быть очень высокими, если нарушения безопасности системы выявляются с большим опозданием.

— Риски, обусловленные умышленными действиями или неумышленным некорректным поведением, могут возникать в случае несанкционированных вторжений в помещения, требующие защиты, или в случае взлома служебных прикладных программ[5].

- **Безопасность на разных стадиях (доступа, операции)**

— Кредитовые переводы предусматривают несколько стадий: доступ пользователя в систему, исполнение платежного распоряжения и выполнение обратной операции. Важно, чтобы меры безопасности, определенные и реализуемые участниками, распространялись на все стадии.

— Поскольку плательщик может направить платежное распоряжение провайдеру платежных услуг в бумажном или электронном виде, используя различные каналы связи (сеть Интернет, мобильную и телефонную связь и т.п.), важно убедиться, что распоряжение передается безопасным способом и обеспечиваются его надлежащая аутентификация и проверка. В противном случае возможны несанкционированные операции.

— Используемая плательщиком процедура передачи платежного распоряжения провайдеру платежных услуг должна обеспечивать конфиденциальность, целостность и доступность деталей распоряжения, а также идентификацию личности инициатора платежа (плательщика). Нарушение конфиденциальности может привести к тому, что незаконно полученные данные будут использованы для мошеннических действий в этой системе.

— Технические сбои или криминальные действия, основанные на обмане, могут привести к несанкционированной операции кредитового перевода с последующими финансовыми потерями одной или более сторон, участвующих в сделке. Причинами подобных рисков могут быть:

  а) процедурный выбор, например, выбор маршрутизации платежных распоряжений между провайдерами платежных услуг;

  б) технические сбои или фальсификации компонентов оборудования или программного обеспечения;

  в) злоупотребления правами доступа[6];

  г) мошенническое поведение сотрудников и/или

  д) то, что мошенники изготовили платежное распоряжение, используя фальшивую или похищенную идентификационную информацию (особенно для дистанционных операций).

  Поскольку системы кредитовых переводов связаны в основном с межбанковскими операциями, внутренние риски (пункты от “а” до “г”) могут представлять особую значимость. Если идентификаторы могут быть похищены (например, логины и кодовые слова для дистанционного банковского обслуживания могут быть получены мошенниками посредством “фишинговых атак” — вида мошенничества в сети Интернет) и повторно использованы, если провайдеры платежных услуг не идентифицируют своих плательщиков должным образом или если платежные распоряжения не проверяются/аутентифицируются, то риск того, что мошенник сможет инициировать несанкционированное платежное распоряжение, будет также весьма значителен.

---

[5] Прикладные программы для управления счетами, обработки платежных распоряжений, переданных по каналам дистанционного банковского обслуживания, или хранения конфиденциальных данных.

[6] В случае осуществления действий неуполномоченными лицами могут возникать риски, связанные с ненадлежащим размещением средств, нарушением конфиденциальности, целостности и секретности данных.

— До тех пор, пока приемлемые меры и средства безопасности не будут использоваться для мониторинга деятельности плательщиков и получателей платежей, будет весьма трудно снизить уровень риска мошенничества. В этом отношении данные, полученные в процессе информационного обмена между подсистемами (например, журналы регистрации и протоколы обработки сообщений и пр.), способны помочь в осуществлении мониторинга деятельности плательщиков и получателей платежей. На основе полученных данных следует принимать меры по снижению уровня подобного риска, например, установить лимиты на операции или обратить особое внимание на операции, превышающие определенную сумму. Это должно осуществляться в соответствии с политиками безопасности системы и ее участников.

— Поскольку кредитовый перевод используется для операций, повторяющихся с определенной частотой, на отдельные дни в течение месяца может приходиться большое количество операций (таких, как регулярные платежи по ипотеке, оплата коммунальных услуг, зарплата, пенсия и др.). Кроме финансовых проблем, связанных с концентрацией этих операций, существует проблема, обусловленная ограниченностью операционных возможностей каждого участника или провайдера в этой системе (например, он может обрабатывать или хранить лишь определенный объем данных). При достижении этого лимита могут возникнуть проблемы доступности и целостности системы в дни пиковой нагрузки.

— Разногласия между участниками нельзя разрешить, не имея прозрачной и легкодоступной информации. При частом возникновении подобных ситуаций будут подорвано доверие к системе и снижена вероятность ее дальнейшего использования.

- **Безопасный клиринг и расчет**

— Проблемы, возникающие в процессе клиринга и расчета, могут вызывать финансовые потери, особенно у провайдеров получателей платежей и/или самих получателей платежей. Это происходит в случае неадекватного обеспечения операционной надежности, безопасности или непрерывности бизнеса. Надлежащий уровень безопасности, операционной надежности и доступности клиринга и расчета в соответствии с уровнем риска и договорными обязательствами (например, предельными сроками расчетов) важен для обеспечения целостности всех данных, участвующих в обмене в рамках клиринга и расчета.

- **Непрерывность бизнеса**

— Катастрофы и события, негативно воздействующие на важные процессы, могут приводить к длительным простоям. Если планы мер по обеспечению непрерывности бизнеса отсутствуют или недостаточно проработаны, могут возникать проблемы, связанные с доступностью, конфиденциальностью и целостностью системы и ведущие к финансовым потерям.

- **Контроль аутсорсинга**

— Если определенные функции системы кредитовых переводов передаются сторонним организациям, то соглашения об оказываемых услугах могут быть недостаточно полными или точными и/или неадекватный мониторинг предоставляемых услуг может вызвать нарушение безопасности. Для обеспечения надлежащего управления аутсорсингом необходимы соглашения с подробным описанием услуг и системы штрафов на случай мошенничества, ошибок при обработке данных или потери доступа в систему.

— Из-за концентрации услуг в руках ограниченного числа внешних поставщиков могут возникнуть серьезные проблемы зависимости от них и проблемы доступности этих услуг.

Стандарт 4. Система кредитовых переводов должна использовать эффективные, контролируемые и прозрачные механизмы системы управления

Ключевые вопросы

4.1. Должны определяться и использоваться эффективные и прозрачные правила и процессы, когда:

— принимаются решения о целях и политике бизнеса, включая политику доступа;

— оцениваются деятельность, удобство и простота использования системы кредитовых переводов;

— выявляются риски, существенные для функционирования системы, принимаются меры по их снижению и предоставляется информация об управлении рисками.

4.2. Следует предусмотреть эффективную систему внутреннего контроля, включающую адекватную и независимую службу аудита.

Пояснительная записка

Ненадлежащее управление может негативно сказаться на системе кредитовых переводов. Для предупреждения, выявления и быстрого реагирования на различные сбои в работе необходимы органы, обеспечивающие эффективные решения и процессы. Чтобы сформировать доверие к системе кредитовых переводов, нужна современная и комплексная политика безопасности. Эффективные процессы внутреннего контроля важны для предотвращения утраты доверия к системе. Без регулирования взаимоотношений и удовлетворения надлежащим образом информационных потребностей участников могут значительно повыситься репутационные риски.

- Участниками системы кредитовых переводов являются провайдеры плательщиков, провайдеры получателей платежей, плательщики и получатели платежей.

  — Адекватные и прозрачные механизмы управления необходимы для того, чтобы орган управления системой кредитовых переводов мог принимать решения должным образом, учитывая потребности всех заинтересованных сторон. Четкая и эффективная связь — это способ обеспечить прозрачность системы. Например, прозрачный доступ предоставляет участникам и клиентам информацию о работе системы кредитовых переводов и обусловленных ею рисках. Он также создает условия для поддержания системой кредитовых переводов динамики рынка и инноваций, регулирования конфликтов интересов, возникающих в силу большого числа участников, а также своевременного и эффективного реагирования в кризисных ситуациях. Для достижения прозрачности следует также сформулировать справедливые критерии доступа в систему и выхода из нее.

  — Для бесперебойного функционирования системы кредитовых переводов важна ее доступность для клиентов. Для развития управления целесообразно оценивать и прогнозировать эволюцию потоков операций, с тем чтобы обеспечивать доступность системы даже в дни пиковой нагрузки. Если орган управления системой кредитовых переводов не получает в явной или неявной форме информацию от клиентов о том, насколько система удовлетворяет их стандарты, то потребности и ожидания клиентов могут оказаться неудовлетворенными. Это также может явиться причиной споров между участниками и/или проблем, обусловленных плохими результатами работы. Должное внимание к этим аспектам поможет сохранить доверие клиентов к системе кредитовых переводов.

  — Эффективные процессы управления рисками способствуют тому, что система кредитовых переводов должным образом предотвращает, выявляет и реагирует на происходящие события. Эффективное управление рисками должным образом учитывает скорость технологических изменений, меняющиеся ожидания клиентуры, распространение угроз и недостатков. Оно также дает возможность выявлять наиболее существенные риски и регулярно информировать о них орган управления системой кредитовых переводов.

- Эффективные процессы внутреннего контроля необходимы для предотвращения и своевременного оповещения о любых сбоях, ошибках или случаях мошенничества, приводящих к потере доверия к системе кредитовых переводов. Анализ внутренних процессов гарантирует быстрое выявление причин ошибок, мошенничества и несогласованности и незамедлительное принятие соответствующих мер по устранению недостатков. Проведение регулярных независимых аудиторских проверок обеспечивает дополнительную уверенность в надежности действующих механизмов.

Стандарт 5. Система кредитовых переводов должна управлять финансовыми рисками, возникающими в процессе клиринга и расчета

Ключевые вопросы

5.1. Система кредитовых переводов должна выявлять финансовые риски, обусловленные клирингом и расчетом, и определять соответствующие меры управления этими рисками.

5.2. Система кредитовых переводов должна обеспечивать, чтобы все выбранные провайдеры клиринга и расчета имели достаточную кредитоспособность, операционную надежность и безопасность.

5.3. Если имеются договоренности о завершении расчетов в случае, когда участник не способен выполнять свои обязательства, необходимо, чтобы его принятые в расчет обязательства не превышали его доступных ресурсов, в противном случае будет поставлена под угрозу его платежеспособность. В соответствии со Стандартом 2 система кредитовых переводов должна также гарантировать полную осведомленность участников об их обязательствах в рамках подобных соглашений.

Пояснительная записка

Завершенность операций кредитовых переводов и финансовая стабильность самой системы могут быть нарушены, если ее орган управления не оценивает (и при необходимости не снижает) финансовые риски, связанные с клирингом и расчетом.

- Неисполнение финансовых обязательств, нарушение в системе безопасности или операционный сбой по вине оператора расчетной системы может привести к значительным, хотя и несистемным, потерям. На это следует обратить особое внимание в том случае, если участники поддерживают положительное сальдо в расчетной системе. Поэтому необходимо регулярно отслеживать кредитоспособность, а также операционную надежность и обеспечение безопасности операторов систем клиринга и расчета.
- Для сдерживания кредитного риска и риска ликвидности могут предусматриваться соглашения о завершении расчетов в случае неспособности участника выполнять свои обязательства. Это приветствуется как с целью снижения финансовых рисков, так и для повышения четкости и определенности потенциальных финансовых рисков для всех участников, особенно в многосторонних системах нетто-расчетов, где реализация рисков может заблокировать цепочку расчетов и/или вызвать непредвиденный дефицит ликвидности.

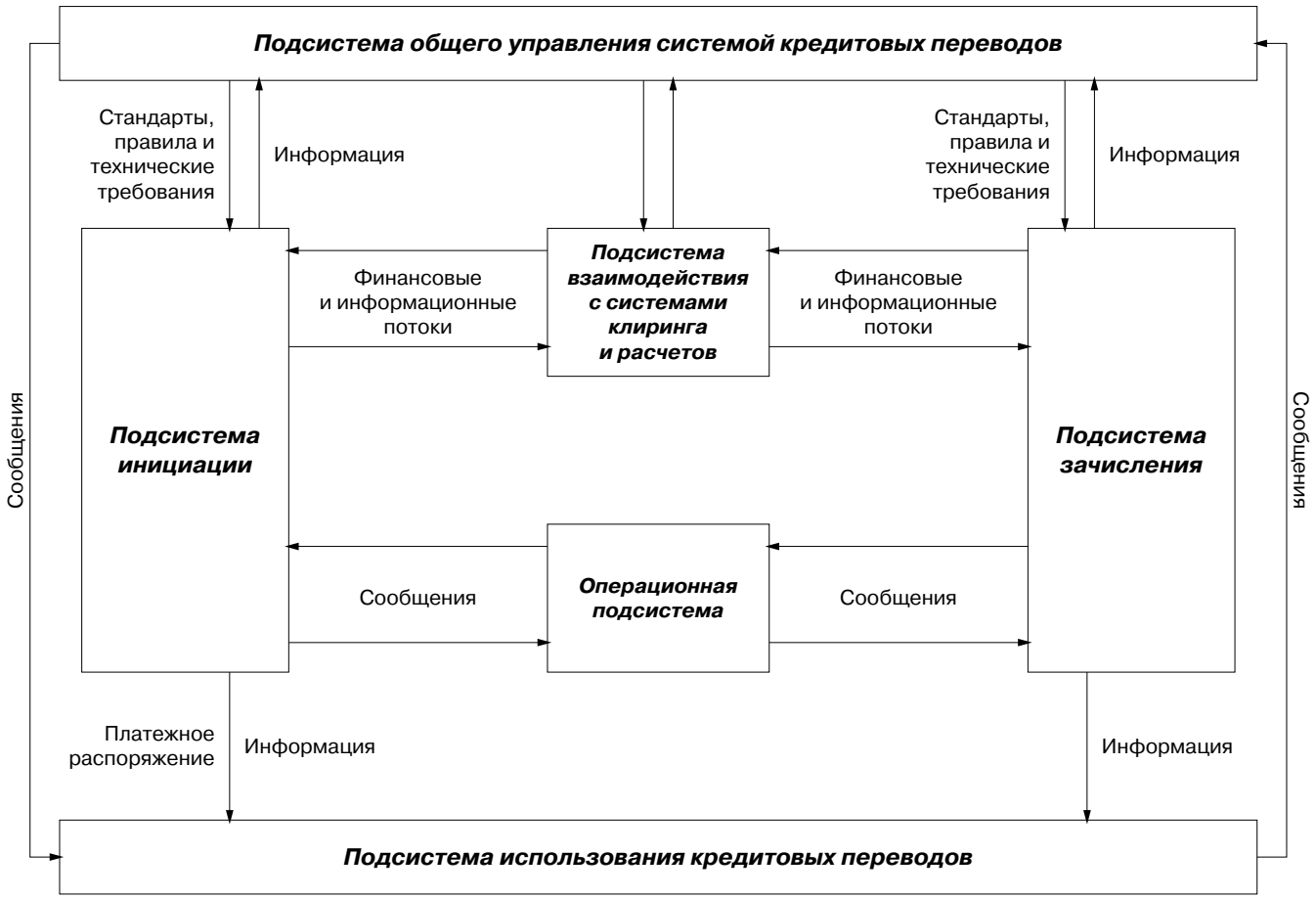
Приложение А
Обзор систем кредитовых переводов

Общая модель

Система кредитовых переводов может быть разделена на шесть компонентов:

1) подсистема общего управления системой;
2) подсистема инициации (подсистема плательщика);
3) подсистема зачисления (подсистема получателя);
4) подсистема использования кредитовых переводов;
5) операционная подсистема;
6) подсистема взаимодействия с системами клиринга и расчета.

Подсистема общего управления системой кредитовых переводов



Различные подсистемы системы кредитовых переводов описаны ниже. Подсистемы представлены с учетом выполняемых задач, а не физических элементов или организаций, которые их осуществляют. Следует пояснить, что в рамках каждой подсистемы несколько организаций могут выполнять взаимосвязанные задачи. Например, в подсистеме инициации платежа могут участвовать и другие организации, помимо провайдера платежных услуг плательщика. И платежные распоряжения, и средства, указанные в них, передаются от провайдера платежных услуг плательщика провайдеру платежных услуг получателя платежа, возможно, через нескольких других провайдеров платежных услуг. Физическое лицо или организация могут выполнять более одной роли в рамках системы кредитовых переводов, например, провайдером платежных услуг плательщика и провайдером платежных услуг получателя платежа может быть одна и та же организация, или одно лицо может быть одновременно плательщиком и получателем платежа.

Подсистема общего управления отвечает за управление (например, определение и распределение прав и обязанностей, подготовку юридически значимых соглашений, разработку стандартов, правил, технических требований или отбор и одобрение уже существующих, а также политик доступа в систему, конкуренции, ценооб-

разования, предотвращения мошенничества, управления, мониторинга деятельности, соблюдения стандартов, решения спорных вопросов и т.д.

Она также отвечает за выработку стратегических планов развития и обеспечение общего взаимодействия с другими системами. Например, в системе кредитового перевода SEPA большинство этих функций выполняет Европейский платежный совет (EPC) (Пленарный комитет или Подкомитет управления схемой кредитовых переводов).

Подсистема инициации включает, в частности, процессы передачи, приема и проверки инструкций кредитового перевода провайдером платежных услуг плательщика (организацией, обслуживающей счет плательщика). Инструкция передается любым согласованным между плательщиком и его провайдером платежных услуг способом. Подсистема инициации обменивается информацией с подсистемой зачисления через подсистему взаимодействия с системами клиринга и расчета (финансовый и информационный потоки) и операционную подсистему (обмен сообщениями).

В *подсистеме зачисления* провайдер платежных услуг получателя платежа получает сообщение о кредитовом переводе, проверяет финансовое и информационное сообщение о кредитовом переводе, кредитует счет получателя платежа и передает должную информацию получателю платежа. Провайдер платежных услуг получателя платежа — организация, обслуживающая счет получателя платежа. Подсистема зачисления обменивается информацией с подсистемой инициации через подсистему взаимодействия с системами клиринга и расчета (финансовый и информационный потоки) и операционную подсистему (обмен сообщениями).

Подсистема использования распространяется на платежные взаимоотношения между плательщиками и получателями платежей (включая информацию, связанную с идентификацией их счетов), а также между ними и их провайдерами платежных услуг (например, правила использования системы кредитовых переводов, отчетность об исполнении/отклонении платежного распоряжения). В этой подсистеме плательщик составляет распоряжение о кредитовом переводе, которым он дает разрешение на выполнение платежной операции.

Подсистема взаимодействия с системами клиринга и расчета относится ко всему объему деятельности и инфраструктуре, необходимых для двустороннего или многостороннего клиринга и расчета по операциям. В рамках системы кредитовых переводов могут использоваться различные системы клиринга и расчета.

Операционная подсистема предоставляет технические или организационные услуги, которые могут быть общими для участников системы кредитовых переводов. Она включает, например, услуги телекоммуникационных сетей, позволяющих обмениваться информационными данными между провайдером платежных услуг получателя платежа и провайдером платежных услуг плательщика (например, платежные распоряжения, возвраты или отказы и информационный обмен другими сведениями, например о случаях мошенничества)[7].

[7] Услуги, оказываемые операционной подсистемой, могут также включать назначение специфических идентификаторов для плательщиков и получателей платежей.

Приложение Б
Глоссарий терминов и определений

В разных системах кредитовых переводов существует разная терминология. Применяемые в настоящем документе определения соответствуют, насколько это возможно, определениям, изложенным в "Директиве по платежным услугам"[8] и применяемым Европейским платежным советом. В данном документе использовались следующие определения:

Аутсорсинг (outsourcing) — положение, когда провайдер услуг привлекает по договору третью сторону для выполнения своих обязанностей в системе кредитовых переводов. Каждый провайдер несет полную ответственность за осуществляемую за него деятельность по договору об аутсорсинге. Провайдер услуг должен обеспечить, чтобы все работы по аутсорсингу управлялись и контролировались так, как будто они были выполнены им самостоятельно.

Возврат средств (return) — результат невозможности зачислить средства получателю провайдером платежных услуг получателя после межбанковских расчетов.

Клиенты (customers) системы кредитовых переводов — это стороны сделки — получатель платежа и плательщик, — пользующиеся услугами системы кредитовых переводов.

- **Получатель платежа (payee)** (или кредитор) — физическое или юридическое лицо — предполагаемый получатель средств по операции кредитового перевода.
- **Плательщик (payer)** (или дебитор) — физическое или юридическое лицо, направляющее платежное распоряжение своему провайдеру платежных услуг инициировать кредитовый перевод.

Клиринг и расчет (clearing and settlement phase) — стадия, включающая в себя весь объем деятельности, необходимой для осуществления двустороннего или многостороннего клиринга и расчета по операциям кредитовых переводов.

Операционная стадия (transaction phase) — процесс исполнения платежного распоряжения посредством кредитового перевода (обычное исполнение или обратная операция), начиная с приема к исполнению платежного распоряжения о кредитовом переводе, инициированного плательщиком, до зачисления средств на счет получателя.

Отказ от исполнения (reject) — результат невозможности выполнить перевод средств по причине отказа от исполнения распоряжения о кредитовом переводе до момента межбанковских расчетов.

Платежный счет (payment account) — счет, используемый для выполнения платежных операций.

Провайдеры платежных услуг (payment service providers) — согласно PSD это: (а) кредитные организации; (б) учреждения, осуществляющие операции с электронными деньгами; (в) почтовые жироорганизации[9]; (г) платежные учреждения; (д) Европейский центральный банк и национальные центральные банки, действующие не в качестве монетарных властей или других государственных органов, и (е) государства — члены ЕС или их региональные или местные органы, действующие не в качестве государственных органов власти.

- **Провайдер платежных услуг плательщика (payer's payment service providers)** — провайдер платежных услуг, открывший платежный счет плательщику и заключивший соглашение с плательщиком о правилах и условиях предоставления продукта с помощью системы кредитовых переводов. На основе этого соглашения он каждый раз выполняет платежные распоряжения плательщика о кредитовом переводе путем их передачи провайдеру платежных услуг получателя.
- **Провайдер платежных услуг получателя платежа (payee's payment service providers)** — провайдер платежных услуг, который открыл платежный счет получателя и заключил с ним соглашение о правилах и условиях предоставления продукта с помощью системы кредитовых переводов. На основе этого соглашения он зачисляет средства на счет получателя на основе информации о кредитовом переводе, полученной от провайдера платежных услуг плательщика.

Система кредитовых переводов (credit transfer scheme) — набор функций, процедур, соглашений, правил и инструментов на бумажном и электронном носителях, которые позволяют исполнять платежные распоряжения, направляемые плательщиком своему провайдеру платежных услуг с целью перевода средств под управление получателя. Перевод средств осуществляется путем дебетования и кредитования счетов незави-

[8] "Директива 2007/64/ЕС Европейского парламента и Совета ЕС" от 13 ноября 2007 года о платежных услугах на внутреннем рынке.
[9] Почтовые организации, оказывающие ограниченные банковские услуги, в т.ч. услуги по приему и осуществлению розничных платежей.

симо от способа, которым плательщик предоставил средства (плательщик может иметь средства на счете или предоставить их наличными).

Стадия доступа (access phase) означает доступ участников (провайдеров или клиентов) в систему.

Участники (actors) системы кредитовых переводов — органы управления, провайдер плательщика, провайдер получателя платежа, провайдеры услуг (в частности, для операционной подсистемы и подсистемы клиринга и расчета), клиенты (получатель платежа и плательщик).

R-операции (R-transactions), или обратные операции, — общий термин для операций отклонения платежного распоряжения или возврата средств. Возможные причины обратных операций включают, помимо прочего, закрытие/блокировку счетов, неверное указание идентификаторов банков и получателя средств в платежном распоряжении, требования органа, осуществляющего надзор и наблюдение.

Центральный банк Российской Федерации

П Р С

Платежные и расчетные системы

Международный опыт

Выпуск 21

Стандарты наблюдения
за европейскими розничными
платежными системами

Наблюдение за платежными схемами,
функционирующими
с использованием карт.
Стандарты

Наблюдение за системами
прямого дебета.
Стандарты

Наблюдение за системами
кредитовых переводов.
Стандарты

2010