СТАНДАРТ ТРИБУНА

E-payments Russia 2013

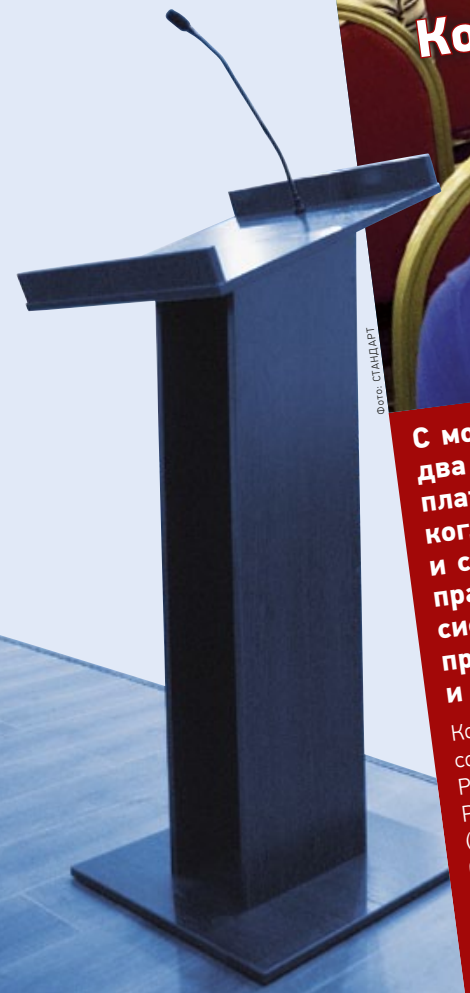

Фото: СТАНДАРТ

С момента вступления в силу ФЗ «О национальной платежной системе» прошло два года, однако закон до сих пор вызывает у участников рынка электронных платежей множество вопросов. Процесс гибридизации платежных продуктов, когда к банковской карте привязываются различные электронные кошельки и счет мобильного телефона, сильно затрудняет регулирование. Участники практической конференции «E-payments Russia 2013 – Электронные платежные системы, мобильные платежи и сервисы в России» обсудили наиболее острые проблемы, связанные с развитием рынка электронных платежных систем и сервисов в стране.

Конференцию поддержали: Ассоциация GSM (GSMA), некоммерческое партнерство «Национальный платежный совет» (НП «НПС»), Ассоциация «Электронные деньги», Ассоциация компаний интернет-торговли (АКИТ), Российская ассоциация электронных коммуникаций (РАЭК), Международная академия связи (МАС), Российский микрофинансовый центр (РМЦ), Национальное партнерство участников микрофинансового рынка (НАУМИР), Всероссийский союз страховщиков (ВСС), Ассоциация профессионалов в области информационной безопасности (RISSPA), Ассоциация участников «МастерКард», Ассоциация региональных операторов связи (АРОС), ГК «Информзащита», ЗАО «Технологии качества» (A1QA), ЗАО «ХроноПэй» (ChronoPay), ООО «ПэйОнлайн Систем» (PayOnline System), ЗАО «Юридическая фирма «Клифф», ООО «КФЦ-Процессинг» («Деньги Online»), ООО «Винус» (PinPay Express), ООО «Удобный маршрут» и ЗАО «Андэк».

Лояльность к карману

Екатерина ЛАШТУН

В условиях стагнации российской банковской системы финансовые учреждения выходят на новый для них рынок электронных платежей. Количество эмитированных банковских карт в стране превысило 160 млн штук, и интернет-эквайринг может стать наиболее перспективным способом осуществления онлайн-платежей в РФ.

В начале сентября 2013 года ComNews провел практическую конференцию «E-payments Russia 2013 – Электронные платежные системы, мобильные платежи и сервисы в России».

«Несмотря на то что с момента вступления в силу ФЗ №161 «О национальной платежной системе» прошло уже два года, закон до сих пор вызывает у участников рынка электронной коммерции множество вопросов», – отметил председатель совета Ассоциации «Электронные деньги», директор по новым платежным технологиям ОАО «Банк «Таврический» Виктор Достов. Он уточнил, что нет четкого разграничения понятий «электронные деньги», «бонусные карты», «транспортные карты» и premium SMS. «Также отсутствует точное определение понятия «интернет-банк», – считает генеральный директор аналитического агентства Markswebb Rank & Report Алексей Скобелев. Он добавляет, что не имеют разграничения как названия и функции, так и платформы и провайдеры услуги. Алексей Скобелев в этой ситуации рекомендует банкам продавать не услугу подключения к интернет-банку, а возможности (например, легкое управление деньгами), делать не платежную систему, а интернет-банк, а также создавать продукты под конкретные потребности клиентов. По словам Виктора Достова, гибридизация платежных продуктов сильно затрудняет регулирование. Они становятся все сложнее: к банковской карте привязываются счет мобильного телефона, мобильный кошелек, кошелек «Яндекс.Деньги» и др. «Кто в этом «колесе» должен отвечать за интересы клиента – непонятно», – недоумевает Виктор Достов. Он называет основные проблемы регулирования в области электронной коммерции: описательный подход в ущерб аналитическому, попытки установить исключения, чрезмерное регулирование, а также озабоченность регулятора незначительными вопросами.

По мнению директора по правовым вопросам ООО «НКО «Яндекс.Деньги» Татьяны Алексеевой, итогами двухлетнего действия ФЗ №161 стали легализация электронных денег (ЭД), появление новых игроков и услуг на рынке, развитие в России рынка электронной коммерции. «Несмотря на положительную динамику, остаются проблемы толкования закона и его правоприменения», – считает она. К основным подводным камням регулирования Татьяна Алексеева относит лимит остатка (оператор электронных денежных средств (ЭДС) не осуществляет перевод ЭДС, если в результате него будут превышены лимиты), лимит оборота (общая сумма ЭДС, переводимых с использованием одного неперсонифицированного электронного средства платежа (ЭСП), не может превышать 40 тыс. рублей в течение календарного месяца), предоставление ЭД оператором (оператор ЭДС не вправе предоставлять клиенту денежные средства для увеличения остатка ЭДС и осуществлять выплату любого вознаграждения клиенту), а также удаленную идентификацию (отсутствует возможность идентификации

Фото: СТАНДАРТ

По мнению директора по правовым вопросам ООО «НКО «Яндекс.Деньги» Татьяны Алексеевой, несмотря на положительную динамику рынка электронных денег в России, остаются проблемы толкования и правоприменения ФЗ №161

Коммерческий директор ООО «ПэйОнлайн Систем» Борис Кривошапкин считает, что банкам гораздо выгоднее не запускать интернет-эквайринг самостоятельно, а отдать этот непрофильный вид бизнеса на аутсорсинг

Фото: СТАНДАРТ

По словам председателя совета директоров НП «НПС» Андрея Круглова, количество банковских услуг в России растет, однако процент платежеспособного населения в стране не меняется

Фото: СТАНДАРТ

Основные цели атак киберпреступников

Источник: Trustwave Global Security Report 2013

клиентов вне мест присутствия оператора). «Тем не менее регулирование рынка ЭДС не стоит на месте, и в первом чтении принят проект Федерального закона №185938-6 «О внесении изменений в статьи 7 и 10 Федерального закона «О национальной платежной системе», – подчеркнула Татьяна Алексеева. По ее словам, этот проект предусматривает пополнение ЭД переводом, в том числе от третьих лиц, предоставление ЭД в случае изменения курсовой разницы, переводы от юридических лиц неидентифицированным клиентам, расширение способов возврата остатка, увеличение лимита остатка для идентифицированных клиентов, возможность частичного исполнения распоряжения о пополнении в случае превышения лимита.

По словам председателя совета директоров НП «Национальный платежный совет» (НПС) Андрея Круглова, в России возникла очень неприятная для экономики вещь – стагнация банковской системы, поскольку все кредитные организации предлагают практически идентичные продукты. «Количество банковских услуг растет, однако процент платежеспособного населения в стране не меняется», – отметил он. Так, в России эмитировано уже более 160 млн банковских карт и многие граждане имеют по нескольку счетов. Поэтому Андрей Круглов полагает, что расширение бизнеса одного банка возможно лишь за счет «отъема» клиентов у другого. «Клиент больше не лоялен к бренду, он лоялен только к своему карману», – уверен Андрей Круглов.

Коммерческий директор ООО «ПэйОнлайн Систем» (PayOnline System) Борис Кривошапкин рассказал, что, поскольку конкурировать напрямую банкам становится все труднее, финансовые организации выходят на новый для себя рынок электронных платежей. Так, в прошлом году оборот рынка интернет-эквайринга (оплата банковскими картами через Интернет) в РФ составил 170 млрд рублей. «В России интернет-эквайринг является наиболее перспективным способом осуществления онлайн-платежей. Количество клиентов, применяющих этот способ расчетов, постоянно увеличивается», – говорит Борис Кривошапкин. Он добавляет, что, для того чтобы оказывать услуги интернет-эквайринга, кредитному учреждению требуются защищенные, масштабируемые технологические и сервисные площадки, сертификация по PCI DSS для работы с платежами, служба поддержки и расчетный центр. Основной причиной, по которой банки не стремятся запускать эквайринг самостоятельно, является высокая стоимость внедрения (10-15 млн рублей) и владения (3 млн рублей в месяц), а также внедрение новых технологий в бизнес-процессы. Кроме того, это нетиповой для банков бизнес. Поэтому представитель PayOnline System рекомендует передавать данный вид услуг на аутсорсинг.

«Кредитное учреждение может использовать интернет-эквайринг как основу для кросс-продаж на быстро растущем рынке», – также сообщил Борис Кривошапкин.

Россия, по данным Trustwave Global Security Report 2013, занимает второе место в мире по количеству атак злоумышленников на системы электронных платежей. «Поэтому обеспечение информационной безопасности (ИБ) систем электронных платежей является актуальной задачей, деньги для решения которой в условиях ограниченных бюджетов организациям нужно тратить эффективно», – отмечает начальник отдела департамента консалтинга и аудита ЗАО «НИП «Информзащита» Евгений Афонин. По его словам, 96% систем ИБ российских компаний уязвимы. Евгений Афонин предлагает обратиться к опыту Южной Кореи, где весной этого года банки подверглись массированным кибератакам. После данного инцидента регулятор установил для кредитных организаций страны следующие требования по ресурсному обеспечению ИБ: число ИТ-специалистов должно составлять не менее 5% от числа штатных сотрудников; число сотрудников, обеспечивающих ИБ, должно быть не менее 5% от числа ИТ-специалистов; на обеспечение информационной безопасности должно выделяться не менее 7% бюджета организации. Все финансовые учреждения Сингапура обязаны сообщать контролирующим органам о киберинцидентах и сбоях в работе информационных систем в течение часа после обнаружения киберугроз и/или неисправностей. Кроме того, подав первичный отчет, организация должна подготовить второй, содержащий развернутый анализ инцидента и детальное объяснение вызвавших его причин. Этот отчет должен быть подан в Денежно-кредитное управление Сингапура (MAS) в течение 14 дней. «Решением проблемы обеспечения ИБ в кредитном учреждении может быть внедрение системы управления рисками информационной безопасности (СУРИБ)», – полагает Евгений Афонин. СУРИБ, по его словам, позволяет идентифицировать, оценивать в стоимостном выражении и приоритизировать риски ИБ, планировать способы их обработки, а также обосновывать ИБ/ИТ-бюджеты. Также система дает возможность производить документирование процедуры управления рисками, выполнение первичной оценки рисков, оформление декларации о применимости механизмов контроля, подготовку проектов планов обработки недопустимых рисков и разработку прототипов средств автоматизации.

Фото: СТАНДАРТ

Андрей Емелин,
президент НП «Национальный платежный совет»

Поправки к ФЗ «О национальной платежной системе»

Отмечу важность внесения поправок в Федеральный закон РФ от 27 июня 2011 года №161-ФЗ «О национальной платежной системе». Этот закон, регулирующий рынок предоплаченных карт, был принят два года назад и в связи с изменениями на рынке электронных платежей требует уточнения редакции ряда статей. Например, в части регулирования электронных денежных средств (ЭДС), подготовки законодательной базы для функционирования системы фрод-мониторинга и регламентации процедур приостановления и возврата несанкционированных переводов. Эти и другие перспективные проекты мы обсуждаем в рамках НП «НПС» и выносим на рассмотрение Госдумы. К сожалению, в этом законопроекте не удалось урегулировать вопрос по сроку проведения перевода ЭДС (ст. 13 «Требования к деятельности оператора электронных денежных средств при увеличении остатков электронных денежных средств физических лиц – абонентов оператора связи»). Законопроект не предусматривает, в течение какого срока этот перевод должен осуществляться, поскольку продолжает сохраняться общее исключение из стандартного трехдневного срока. Очевидно, что сохранение такого исключения неудобно как для оператора ЭДС, так и для абонентов. Поэтому мы согласовали позицию о целесообразности установления трехдневного срока, в том числе для перевода ЭДС, и довели ее до сведения Госдумы. Речь идет о любых переводах, не только операций, совершающихся в автономном режиме.

Второй момент, который мы также посчитали важным отразить в этом законопроекте, – вопрос регулирования взимания комиссии для осуществления перевода ЭДС. Пока основной моделью остается взимание комиссии с плательщика. В ситуации, когда плательщик не имеет счета у оператора, осуществляющего перевод ЭДС, проблема взимания комиссии встает чрезвычайно остро. В законе есть оговорка, предусматривающая возможность взимания комиссии с получателя, однако не прописаны подробно процедуры для этой ситуации, что, по нашему опыту, вызывает в ряде случаев непонимание у участников рынка и даже у регулятора. В связи с этим мы сформировали и предложили Госдуме внести поправку, которая касается прямого регулирования возможности взыскания комиссии с получателя, при этом наши предложения были дополнены положением о том, что основное обязательство плательщика будет считаться исполненным в полной сумме перевода, который он осуществил. Таким образом, на стороне плательщика ничего не меняется, а на стороне получателя будут применены модели, которые широко распространены и прекрасно себя зарекомендовали. Определенное негативное влияние на применение модели взимания комиссии с получателя оказывает ограничение взимания комиссии при оплате услуг ЖКХ. Однако другую модель придумать невозможно, а за операцию в любом случае кто-то должен платить, и это должно быть заинтересованное лицо. В ситуации с массовыми незначительными по сумме платежами это оптимальное решение, и оно требует прямого регулирования в законе.

Одна из инициатив, оформление которой мы сейчас завершаем, направлена на совершенствование и упрощение расчетов с ЭДС. Это проект стандарта по штрихкодированию данных о получателе платежа, он разработан при активном участии крупнейших банков. Так, основные ресурсоснабжающие организации широко применяют различные виды штрихкодов, и мы считаем важным официально закрепить в качестве рекомендуемых три двухмерных стандарта, наиболее распространенных на рынке. Мы понимаем, что существуют поставщики, которые используют одномерные стандарты, поэтому предусмотрели оговорку, что в течение определенного переходного периода они смогут их применять. Такая унификация позволит значительно ускорить продвижение данного инструмента в массы, и новые поставщики будут сразу ориентироваться на использование установленных технологий. Это ускорит работу банков на уровне офисов, а также упростит работу с информацией, хранящейся на электронных носителях при дистанционном взаимодействии с клиентами. С темой безопасного и точного донесения информации до банка тесно связан вопрос безопасной работы с ЭДС. Поэтому мы готовим памятку для потребителя по использованию ЭДС и в ближайшее время предложим ее в качестве стандарта.

Фото: СТАНДАРТ

Елена Денисова,
руководитель коммерческой практики гражданско-правового департамента ЗАО «Юридическая фирма «Клифф»

Единые карты оплаты и совместные бонусные программы: правовой аспект

Единая карта оплаты – продукт интересный, получивший за последний год широкое распространение на российском рынке. Такие карты, в отличие от множества карт для разных целей, очень удобны для пользователя, однако с правовой точки зрения с ними связано множество вопросов. Так, в законе отсутствует понятие «единая карта оплаты». Есть инструкция Банка России, вступившая в силу с 1 июля 2013 года, в ней говорится о платежных картах. Банковская карта, согласно этой инструкции, теперь относится к виду платежной карты. Далее Центробанк (ЦБ) выпустил письмо с информацией о том, что некредитные организации стали эмитировать бонусные карты. Ситуация для 2013 года выглядит странно, поскольку бонусные карты выпускаются на российском рынке как минимум с 2010 года. Следом вышла очередная инструкция ЦБ, в которой он прямо указал на то, что все бонусные накопительные карты, которые позволяют расплачиваться в партнерских сетях за товары и услуги, являются платежными картами. А платежные карты, согласно ФЗ №161 «О национальной платежной системе», могут быть эмитированы только кредитными организациями. Обращаю внимание, что это касается лишь тех карт, которые позволяют расплачиваться в нескольких сетях (так называемые партнерские сети). Если бонусная накопительная карта эмитирована для собственных нужд магазина (сети), то она не подпадает под ограничения ФЗ №161.

ЦБ в инструкции предусмотрел несколько видов платежных карт, под которые впоследствии будут подведены бонусные и единые карты. Это кредитные и дебетовые карты (относятся к банковским), а также предоплаченные карты (в ФЗ №161 указано, что такие средства платежа могут быть как персонифицированными, так и неперсонифицированными).

У участников рынка электронной коммерции возникает множество вопросов о том, как можно создать единую платежную карту и имеет ли право компания, не являющаяся кредитной организацией, ее эмитировать. Исходя из инструкции ЦБ, которая является не правовым актом, а лишь позицией, эмиссия такой карты возможна только для оплаты собственных товаров и услуг магазина.

С юридической точки зрения остается непонятным статус бонусных и накопительных карт. Фактически это инструмент программ лояльности, и они должны подпадать под закон «О рекламе». Однако эти карты регулируются ФЗ №161. Налицо конфликт норм права.

Следует учитывать, что, если речь идет о накопительной программе, подразумевающей возможность оплаты в партнерских компаниях (например, карты «Малина» и «Кукуруза»), карты могут эмитировать только кредитные организации. Сегодня единственная организация, которая отвечает этим признакам на 100%, – ОАО «Сбербанк» (карта «Спасибо»).

Если карта предполагает получение неких бонусов за действие, то она не подпадает под действие ФЗ №161, поскольку не подразумевает выплаты денежных средств. Таким образом, основной признак того, подпадает ли карта под действие ФЗ «О национальной платежной системе», – возможность использования электронных единиц (баллов) в качестве оплаты. Подчеркну, что снижение стоимости (скидки на товары и услуги) также является оплатой.

Организации, желающей эмитировать единые карты оплаты или бонусные карты, следует выполнить минимум два требования, установленных законом «О рекламе» и ФЗ №161. Во-первых, разработать правила проведения акции (как будет происходить эмиссия карт и каким образом будет осуществляться их учет). Если компания предусмотрела денежные выплаты, то ей необходимо договориться с кредитным учреждением о выпуске банковских карт. Если выплат не будет, то достаточно обычных правил проведения акции. Во-вторых, компании необходимо стать оператором обработки персональных данных и разместить в общем доступе соответствующие правила. Но даже соблюдение всех требований не избавит организацию от пристального внимания со стороны ЦБ, поскольку каждая бонусная программа и единая карта оплаты, подразумевающие выплату электронных денежных средств, находятся под его особым контролем.

Фото: СТАНДАРТ

Илья Сачков,
генеральный директор ООО «Группа информационной безопасности» (Group-IB)

Компьютерная преступность в России

Компания Group-IB осуществляет предотвращение экономических и высокотехнологических преступлений в России, США и Азии. Около 80% обвинительных заключений по российским компьютерным преступникам – дело рук наших криминалистов и экспертов. Оборот рынка киберпреступности на территории РФ впечатляет: он уже обогнал объем рынка наркотических веществ и с каждым годом увеличивается. Вследствие бурного развития интернет-банкинга и платежных систем новые сервисы использует огромное количество физических и юридических лиц без базовых знаний основ информационной безопасности. Инциденты, связанные с системами дистанционного банковского обслуживания (ДБО), происходят как в небольших, так и в крупнейших российских компаниях.

Приведу простой пример, как выглядит со стороны злоумышленника ботнет. Система управления ботнетом и системой ДБО по краденым пользовательским данным представляет собой отнюдь не зеленый экран, который часто фигурирует в кинофильмах про хакеров, а достаточно удобный интерфейс. Наверху представлены платежные системы, которые используют злоумышленники, далее идут украденные данные и ключи.

Стоимость создания вредоносного программного обеспечения составляет около $500 тыс., с его помощью можно сделать практически все что угодно: заблокировать и нарушить действия загрузочной системы. В этом году мы расследовали инцидент, когда российский киберпреступник сумел за пару недель осуществить 13 тыс. заражений компьютеров, на которых использовалась та или иная платежная система. Это не просто зараженный компьютер физического лица. Вредоносное ПО определяет, использует ли компьютер платежные системы, и только тогда атакует его.

Вера в то, что российские киберпреступники – патриоты, ни на чем не основана. На территории РФ огромное число клиентов банков, которые пользуются интернет-сервисами, их легко заразить из-за несовершенства операционных систем, браузеров и настроек программ обновлений. Кроме того, в стране существует определенная безнаказанность. Поэтому россияне являются лакомым кусочком для хакеров. Основное отличие отечественной киберпреступности в том, что у нас до сих пор существует такое экономическое преступление, как обналичка денег. Из-за киберпреступников ее сроки сократились до одного дня.

Характерно, что за последний год кибермошенники стали ленивыми, и теперь они тщательно выбирают счета, с которыми будут работать. Так, минимальная сумма, которая может их заинтересовать, составляет около 300 тыс. рублей. Злоумышленники, работающие с меньшими суммами, обычно новички и быстро выходят из дела в результате заведения на них уголовных дел, или же их берут в оборот более опытные преступники из других группировок.

Многие интернет-пользователи сомневаются в возможности кражи электронно-цифровой подписи (ЭЦП), поскольку она хранится на USB-носителе или защищена с помощью двухфакторной SMS-аутентификации. Однако киберпреступники с легкостью взламывают ЭЦП. Как только находится ключ в компьютере, для злоумышленника нет абсолютно никакой разницы, где находится ЭЦП, поскольку вредоносное ПО уже заразило этот компьютер. Платежное поручение отправится прямо с него в руки злоумышленника в момент использования ЭЦП в результате подмены реквизитов. Что касается SMS-авторизации, в реальности пользователь отправляет сообщение не для аутентификации, а для совершения других операций. Большинство банков, внедривших двухфакторную SMS-аутентификацию для интернет-банкинга в надежде остановить хищения, столкнулись с этим еще в конце 2012 года.

Тенденцией начала 2013 года являются целевые атаки на компьютеры операционистов банков и сотрудников, отвечающих за выдачу ЭЦП. В этом случае злоумышленник получает возможность перевыпустить любые ЭЦП для клиентов банка. Только за I и II кварталы этого года на территории страны произошло 24 целевых заражения компьютеров сотрудников крупнейших банков.

Из-за использования платежных инструментов на мобильных телефонах увеличилось количество атак на мобильные устройства, в основном работающие на наиболее распространенной ОС Android.

Фото: СТАНДАРТ

Лев Денисов,
коммерческий директор
ООО «Удобный маршрут»

Перспективы бесконтактных безналичных платежей на транспорте в РФ

Система безналичных платежей «Удобный маршрут» работает в 12 регионах РФ и в трех регионах находится в процессе запуска. Мы оснастили системой свыше 220 пассажирских транспортных предприятий и выпустили более 7 млн бесконтактных карт. Мы также являемся официальным поставщиком карт для ОАО «Универсальная электронная карта», а в сентябре прошлого года начали оказывать услуги оплаты проезда с помощью мобильного телефона. Транспортными бесконтактными картами хотят заниматься многие: операторы, владельцы платежных систем, ОАО «УЭК». Однако прежде следует задать себе вопрос: а в чем выгода? Существует мнение, что система повысит комфорт и удобство пассажиров. Но на практике происходит совсем наоборот: это вызывает дополнительные очереди и давку. Неужели карта может увеличить вместимость автобуса? Конечно, нет. Удобство платежей – это то, что интересует пассажиров меньше всего. Есть также мнение, что безналичная оплата проезда приводит к росту доходов. Одни эксперты называют цифру 30%, другие – 50%. Обычно при этом предлагаются инвестиционные схемы: инвестор, внедрив систему, забирает 7%, 12%, 15% с оборота на покрытие расходов. Схема выглядит привлекательно: пусть даже затраты будут 15%, рост-то все равно составит 30%! Но так ли это? За счет чего произойдет рост? Типовая структура пассажиропотока до внедрения безналичной оплаты выглядит следующим образом: 30-40% льготных категорий граждан, 5-10% покупают билеты заранее, и более 50% приобретают билеты у водителя. Через два года после внедрения системы безналичных платежей ситуация практически не изменилась: все так же около 50% пассажиров приобретают билеты у водителя за наличные средства. Бескондукторная система представляет собой, по сути, систему на доверии. Мы возвращаемся к забытому советскому лозунгу «Совесть пассажира – лучший контролер». Современный вариант лозунга: «Маршрут работает в бескондукторном режиме. Обилечивание самопроизвольное». То есть особых новшеств и не появилось.

Главными вопросами для компаний, внедряющих транспортные карты, стали следующие: Как принять платеж, когда у пассажира нет карты? Как наказывать за неплатежи? Недостатками систем на доверии являются невозможность взимания штрафа на месте, сложность процедуры выписывания штрафа, проблема собираемости штрафов, поступление штрафов в бюджет, а не на предприятия. И наконец, безбилетник рискует только стоимостью разового проезда. Таким образом, закон на стороне безбилетника, а тарифы на транспорт регулируются государством. О каких системах лояльности можно говорить, если себестоимость перевозки выше действующих тарифов?

Отдельно стоит остановиться на NFC-платежах. Удивительно, но флагманские мобильные устройства не поддерживают микросхемы для смарт-карт типа Mifare Classic (де-факто стандарт в системах оплаты проезда). Сотрудники транспортных компаний, например водители, не заинтересованы в безналичном расчете, поскольку в этом случае они лишаются «дополнительного заработка» в виде денег за билеты. Кроме того, льготные категории граждан требуют отдельного учета. Мы решаем эти вопросы по мере сил. За последние пять лет интерес государства к развитию инфраструктуры безналичных платежей на транспорте заметно вырос, поскольку в ее отсутствие не будет ни NFC, ни других перспективных технологий бесконтактных платежей. Наш подход иной, это 100%-ный охват всех категорий пассажиров бесконтактными электронными картами. Платежи производятся наличными средствами, а их учет – электронный. Используются транспортные карты, банковские карты с бесконтактным интерфейсом, универсальные электронные карты, а также мобильные телефоны с поддержкой NFC. Система применима для всех пассажиров, эффект также заметен незамедлительно. Так, после внедрения нашей системы в Ульяновске рост выручки транспортного предприятия составил 26%, а в Чувашии – 30%. Система «Удобный маршрут» обладает современной двухуровневой архитектурой, которая проще в использовании и дешевле в эксплуатации, чем традиционные разрозненные системы. Преимуществами нашего подхода являются сжатые сроки внедрения, минимум капитальных и операционных затрат, решение реальных проблем на транспорте, а также создание инфраструктуры для безналичных платежей.

Евгений Афонин,
начальник отдела департамента консалтинга и аудита ЗАО «НИП «Информзащита»:
«Около 90% российских банков пока не видят негативных последствий вступления в силу с 1 января 2013 года ст. 9 ФЗ №161. Мы считаем, что кредитные учреждения еще не делали оценку возможных проблем. Однако практика показывает, что новое регулирование может вызвать существенное увеличение фрода на рынке электронных денег»

Фото: СТАНДАРТ

Фото: СТАНДАРТ

Алексей Породзинский,
ведущий специалист департамента оптимизации качества программного обеспечения ЗАО «Технологии качества» (A1QA):
«Нагрузочное тестирование является чрезвычайно важным способом оценки уязвимости платежной системы. В процессе тестирования мы изучаем пиковую активность пользователя в различное время. Результаты испытаний позволяют настроить систему таким образом, чтобы исключить риски и избежать ее возможного отказа»

Александр Лиходедов,
начальник отдела дистрибуции Департамента транспорта и развития дорожно-транспортной инфраструктуры Москвы:
«Электронная транспортная карта «Тройка» – это универсальный носитель, который объединит в себе все билеты (на городской транспорт, электрички, аэроэкспрессы, парковки, прокат велосипедов) и повысит удобство пользования общественным транспортом. Важно, что цены проезда по карте «Тройка» зафиксированы до 2015 года»

Фото: СТАНДАРТ

Фото: СТАНДАРТ

Михаил Мамута,
президент Российского микрофинансового центра:
«Принятие ФЗ №161 позволило увеличить доступность финансовых услуг в России, а также упорядочить банковско-агентскую модель взаимодействия. Однако тема мобильных финансовых услуг раскрыта в этом законе очень слабо, и мы считаем, что рынку не хватает подзаконного регулирования в данной сфере»

Фото: СТАНДАРТ

Юлия Белозерова,
менеджер проектов по интеграции платежных систем ООО «КФЦ-Процессинг» («Деньги Online»):
«Темп роста рынка мобильных бизнес-приложений в России в течение следующих четырех лет составит 110% в год. При этом аналогичный показатель по миру – 94%. К 2016 году отечественный рынок мобильных бизнес-приложений увеличится до $62,9 млн. Таким образом, происходит миграция бизнеса на мобильные платформы»

Константин Абрамов,
старший менеджер по развитию бизнеса департамента новых платежных технологий ООО «МастерКард»:
«Платежное средство MasterCard Mobile уже позволяет российским пользователям совершать оплату счетов и выполнять денежные переводы. В будущем мы планируем добавить функции автоматического выставления счетов, погашения кредитов, переводов с карты с возможностью получения наличных средств через сеть операторов денежных переводов»

Фото: СТАНДАРТ

Мнение

Алексей Ковыршин,
генеральный директор ЗАО «ХроноПэй» (ChronoPay):

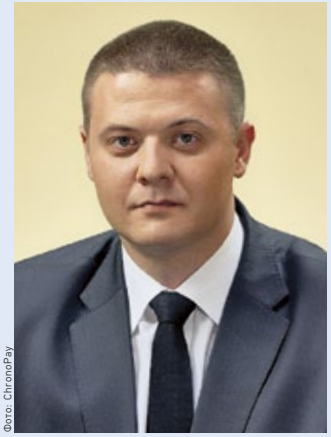

Фото: ChronoPay

«Компания ChronoPay является глобальным оператором интернет-платежей с помощью банковских карт. Мы предоставляем платформу для обработки платежей в Интернете, обеспечивающую возможность принимать к оплате карты международных платежных систем Visa, MasterCard, American Express, Japan Credit Bureau (JCB) и других платежных систем, а также электронные деньги: WebMoney, «Яндекс.Деньги», Qiwi.

Ситуация на российском рынке интернет-эквайринга (услуга, позволяющая принимать банковские карты для оплаты товаров и услуг в Интернете) серьезно поменялась с выходом на него банков. Теперь рынок принадлежит не только традиционным игрокам – эквайерам, таким как наша компания, но и кредитным организациям. Однако у большинства банков пока отсутствует серьезный опыт в области обеспечения информационной безопасности в интернет-эквайринге. Поэтому основные клиенты банков – это компании, бизнес которых не сильно подвержен кибермошенничеству, например из сферы жилищно-коммунального хозяйства. Мошенник не станет оплачивать свой счет за электроэнергию украденной картой, потому что его сразу вычислят.

ChronoPay является одним из первопроходцев на рынке интернет-эквайринга в России. Опыт, накопленный за 10 лет, позволил нам занять лидирующие позиции на этом рынке. Крупные компании, такие как Microsoft, авиакомпания «Трансаэро», «Мобильные ТелеСистемы», «Бегун», потому и работают с нами, что не могут позволить себе доверить бизнес новичкам, у которых нет наработанных знаний в этой области. Мы успешно предотвращаем по нескольку десятков, а то и сотен попыток мошенничества в день. Созданная нами система антифрода при каждой транзакции запускает набор разнообразных фильтров, анализируя помимо стандартных показателей, вроде номера карты, еще и версию операционной системы, часовой пояс и другие параметры. Ежегодно мы успешно проходим проверку на соответствие стандарту PCI DSS, проводимую лицензированным аудитором Visa и MasterCard компанией SRC Security Research & Consulting GmbH. Такой подход позволяет эффективно пресекать попытки мошенничества и пропускать только законные транзакции.»