Белые пятна PCI DSS

Пятиизбянцев Николай Петрович

Payment Card Industry (PCI)

Data Security Standard

Requirements and Security Assessment Procedures

Version 3.1

April 2015

Стандарт применяется для всех организаций сферы обработки платежных данных: торгово-сервисных предприятий, процессинговых центров, банков-эквайеров, организаций, выпускающих платежные карты, и поставщиков услуг, а также других организаций, которые хранят, обрабатывают или передают данные держателей карт и (или) критичные аутентификационные данные.

Список организаций, которые попадают под требования всеобъемлющий и охватывает всю индустрию.

Но реализацией требований Стандарта занимаются платежные системы в рамках своих программ.

В этих программах существуют «белые пятна»:

Участники индустрии платежных карт хранят, обрабатывают, передают данные держателей карт и (или) критичные аутентификационные данные, но под контроль выполнения требований стандарта не попадают.

VISA: Account Information Security.

Эквайрер соответствует требованиям PCI DSS, когда все его торговцы и поставщики услуг (сервис провайдеры) соответствуют PCI DSS.

Торговец (Merchant) – это юридическое лицо, которые в соответствии с подписанным соглашением с эквайрером несет обязательства по приему документов, составленных с использованием платежных карт, в качестве оплаты за предоставляемые товары, работы, услуги.

Поставщики услуг или агенты (agents) – это организации, которые оказывают сервисы, связанные с платежами, прямо или опосредованно клиентам VISA («клиент» – это банк) или их торговцам.

VisaNet процессор:

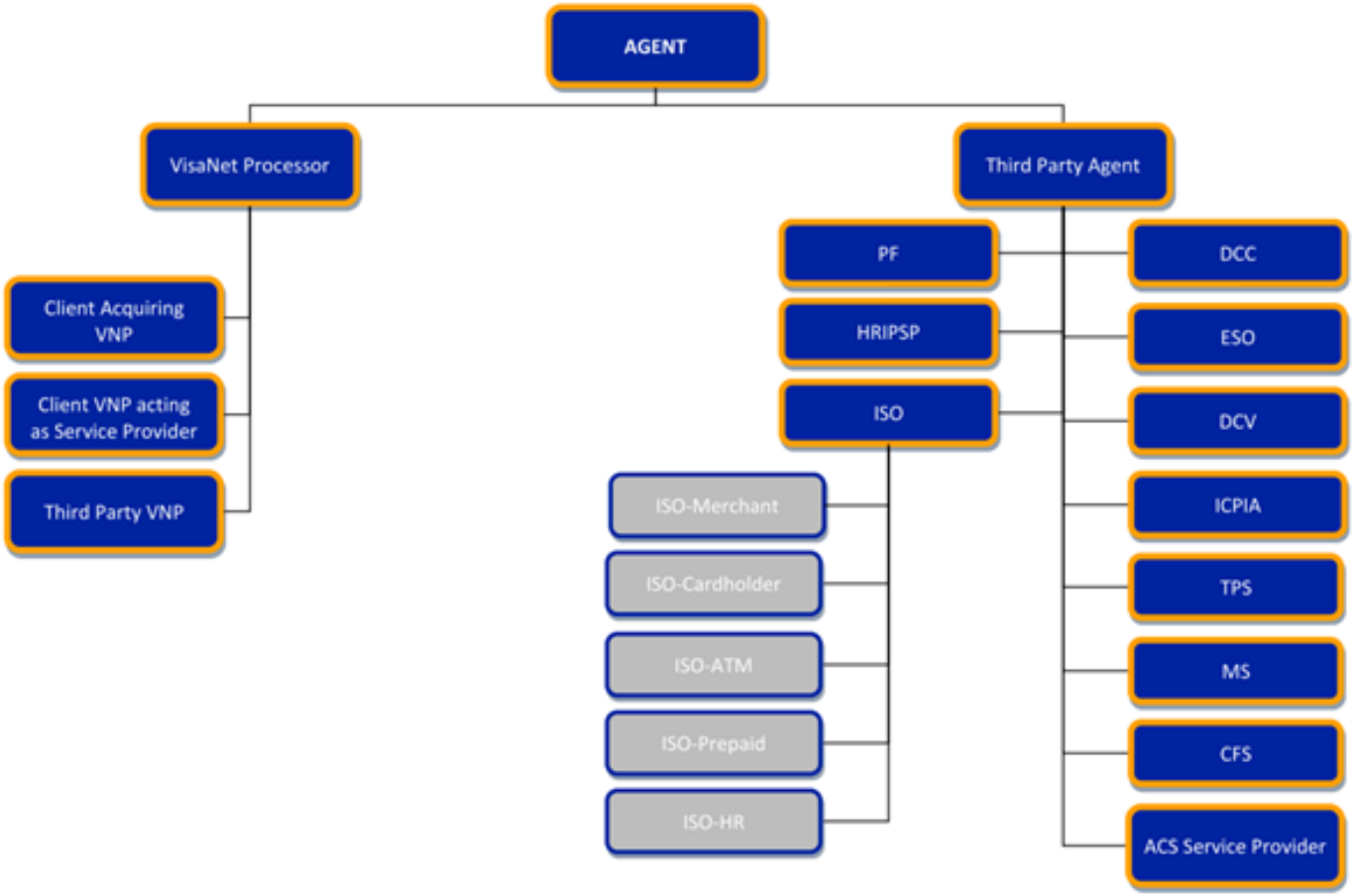
1) Банк эквайрер (Client Acquiring VNP) - подключен напрямую к VisaNet, обрабатывает только эквайринговые транзакции для своих торговцев, под своим, лицензированным для него, БИНом.

2) Банк сервис-провайдер (Client VNP acting as Service Provider) – подключен напрямую к VisaNet, обеспечивают эмиссионные и/или эквайринговые сервисы карточного процессинга для других клиентов Visa, торговцев, которые не обслуживаются им и/или другими по эквайрингу.

3) Сторонний (Third Party VNP) – не банк Visa, подключен напрямую к VisaNet и обеспечивают эмиссионные и/или эквайринговые сервисы карточного процессинга клиентам Visa, торговцам и/или другим поставщикам услуг.

К сервис-провайдерам также относятся независимые агенты (Third Party Agent) – организации, которые не попадают под определение VisaNet процессора, но предоставляют услуги, прямо или косвенно связанные с платежами, клиенту Visa и/или хранят, передают и/или обрабатывают данные держателей карт.

Guide to Visa Inc. Agents



Согласно определениям независимых агентов (TPA), все они должны иметь договорные отношения с банками членами Visa или торговцами.

Следовательно:

Все организации, напрямую подключенные к сети VisaNet, а также другие организации, которые хранят, обрабатывают или передают данные держателей карт и (или) критичные аутентификационные данные и при этом имеют договорные отношения с банками членами Visa или торговцами, попадают под программу контроля требований PCI DSS «Требования и процедуры аудита безопасности» - Account Information Security.

В России есть банки ассоциативные члены платежной системы Visa, которые имеют собственные процессинговые центры, но подключены к VisaNet через полноправных членов (principal member) – процессинговые центры второго уровня.

Такие организации не являются ни VisaNet Processor, ни Third Party Agent, ни тем более Merchant.

Таким образом, они не попадают под программу Account Information Security и контроль выполнения соответствия «Требованиям и процедурам аудита безопасности» PCI DSS в рамках указанной программы не обеспечивается.

Payment Card Industry (PCI)

PIN Security Requirements

Version 2.0

December 2014

Индустрия платёжных карт (PCI)

Требования к защите ПИН

These requirements are intended for use by all acquiring institutions and agents responsible for PIN transaction processing on the payment card industry participants' denominated accounts and should be used in conjunction with applicable industry standards. These requirements do not apply to issuers and their agents.

Данные требования предназначены для использования всеми эквайринговыми организациями и агентами, занимающимися процессингом транзакций с применением ПИН-кодов по счетам участников индустрии платёжных карт, и должны применяться в комбинации с действующими отраслевыми стандартами. Настоящие требования не касаются эмитентов платёжных карт и их агентов.

PIN Program Participants include:

• PIN Acquiring Third-Party VisaNet Processor (VNP) – A third party VNP entity that is directly connected to VisaNet and provides acquiring PIN processing services to members.

• PIN Acquiring Client VNP acting as a Service Provider – A Visa member or member-owned entity that is directly connected to VisaNet and provides PIN acquiring processing services to members.

• PIN Acquiring Third-Party Servicers (TPS) – A third-party agent that stores, processes, or transmits Visa account numbers and PINs on behalf of Visa members.

• Encryption and Support Organizations (ESO) – A non-member organization that deploys ATM, POS, or kiosk PIN acceptance devices which process and accept cardholder PINs and/or manage encryption keys (i.e., key injection facilities (KIFs)).

Банки эквайреры, не являющиеся Third-Party VNP, Client VNP , TPS, ESO не попадают под программу PCI PIN Security и контроль выполнения соответствия данным требованиям не обеспечивается.

Выполнение требований PCI DSS должны обеспечить банки – спонсоры, они несут ответственность за ассоциативных членов (агентов).

Но имеются ли у банка-спонсора реальные механизмы воздействия на агента?

Прямых требований, аналогичных требованиям к торговцам и агентам (сервис-провайдерам) со стороны платежных систем нет. Есть ответственность банка спонсора за своего агента. То есть, если в сети агента произошла компрометация данных держателей карт, то финансовую ответственность будет нести спонсор. На первый взгляд, данное положение должно было бы обеспечить выполнение требований PCI DSS, так как спонсор экономически заинтересован, чтобы агенты соответствовали Стандарту. Но можно ли этого достичь на практике? В сегодняшней ситуации, скорее всего, нет. Максимум чего можно добиться: 1) спонсор рекомендует (а не требует) соблюдение PCI DSS, 2) агент выполняет требования в силу своих финансовых и технических возможностей.

Типовое бизнес-предложение QSA аудитора (начало 2014 г.)

для типовых бизнес-процессов поставщиков услуг категории Level 1, CNP эквайринг, до 20 серверов, 10 ИТ/ИБ специалистов, 3 внешних IP-адресов:

Обследование и рекомендации – 280 т.р.

Разработка документов – 100 т.р.

ASV-сканирование – 22 т.р.

Тест на проникновение – 210 т.р.

QSA-аудит – 280 т.р.

ИТОГО: 892 т.р.

Аудит необходимо проходить ежегодно. При повторных аудитах затраты на обследование, рекомендации и разработку документов сократятся, но после обследования необходимо будет выполнить рекомендации по приведению в соответствие. Что будет так же составлять существенные затраты. Скорее всего, банк агент не захочет (не сможет) нести данные расходы.

Возможно вопрос соответствия PCI DSS банка агента решило бы требование со стороны банка спонсора по заполнению агентом самоопросника?

Но здесь возникает сложная ситуация: если банк ответит на все вопросы «как есть», то, во-первых, это займет с это стороны гораздо больше усилий и времени для выяснения истинного положения дел, а во-вторых, будет вероятность того, что не будет соответствия требованиям стандарта. Если это выясниться, опять встанет вопрос: кто будет платить за приведение системы в соответствие требованиям стандарта? А если банк агент ответит на вопросы «как надо», то сил, времени и финансовых средств это существенно сэкономит. Тем более, что не выполнение хотя бы одного требования Стандарта, означает не соответствие Стандарту в целом.

Банк спонсор не может обязать банк агент соответствовать требованиям PCI DSS, максимум – рекомендует выполнять Стандарт и переложит (в договоре) риски штрафных санкций за компрометацию данных держателей карт на агента.

АО «Национальная система платежных карт»

Операционный платежный клиринговый центр национальной системы платежных карт - ОПКЦ НСПК

Операции по картам международных платежных систем российских банков, осуществленные на территории России должны процессироваться через ОПКЦ НСПК.

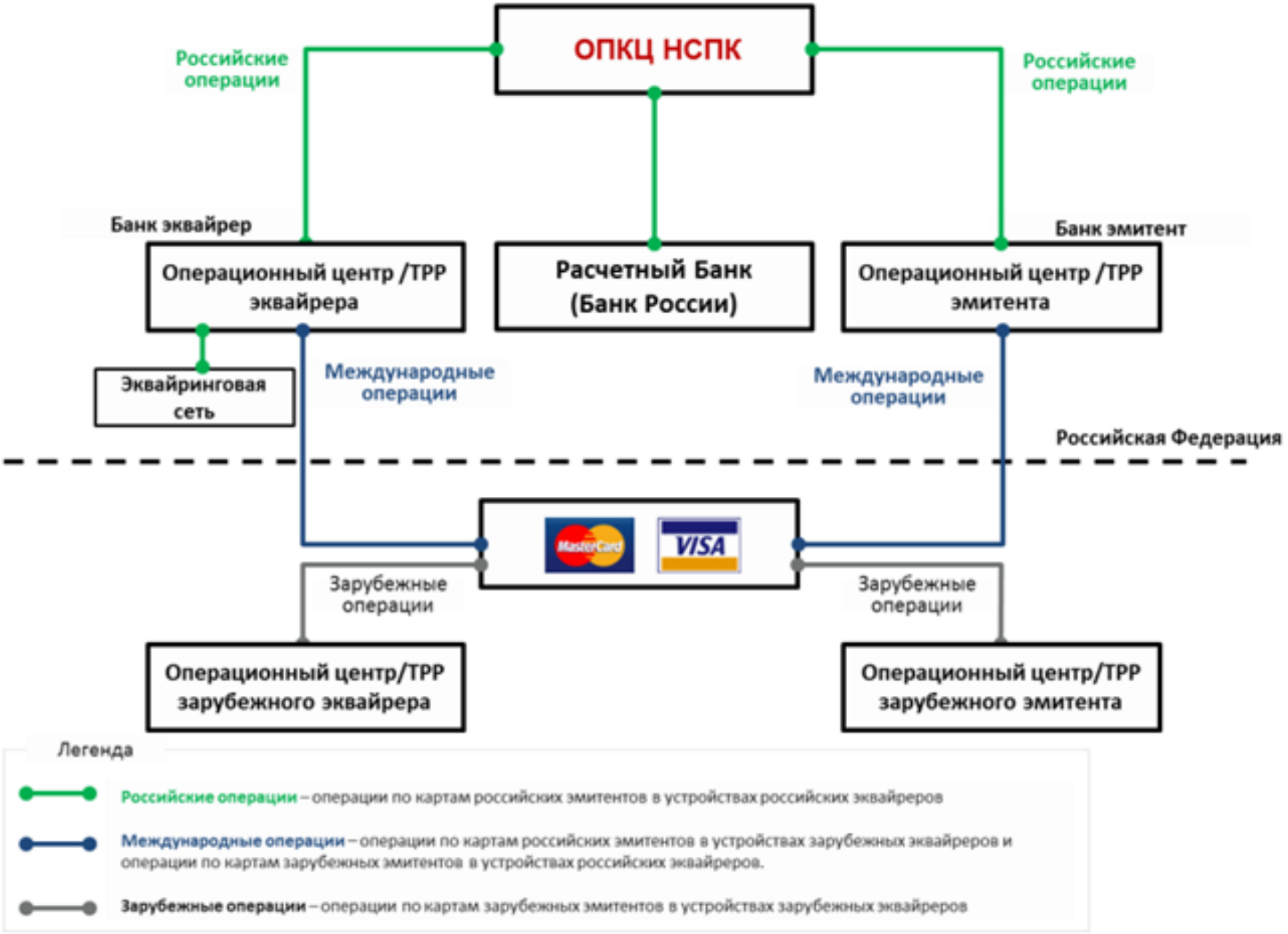
Руководство по подключению и взаимодействию с ОПКЦ НСПК. Часть 2.1. Руководство по операционному взаимодействию с ОПКЦ НСПК по операциям платежной системы MasterCard (Версия 1.0.0. от 22.12.2014)»:

1. Общие положения

Статус ОПКЦ НСПК в платежной системе MasterCard

АО «НСПК» информирует российских Участников MasterCard о том, что MasterCard присвоил АО «НСПК» статус Type 1 Third Party Processor (Type 1 TPP). Настоящий статус действует с 17 ноября 2014 года.

Рисунок 1. Схема взаимодействия операционных центров и процессоров третьей стороны с ОПКЦ НСПК



Если бы ОПКЦ НСПК не только замыкал на себя весь внутрироссийский транзакционный трафик, но и предлагал услуги по подключению через себя к МПС в качестве независимого Processor, то российские банки, которые в настоящий момент подключены к МПС напрямую, могли бы стать процессингами второго уровня и перестали бы попадать под требования аудита по PCI DSS, чем существенно сократили бы свои издержки.

Банки в настоящий момент вынуждены поддерживать два интерфейса: внешний к МПС и внутренний к ОПКЦ НСПК.

Организация ОПКЦ НСПК в качестве единого головного регионального операционно-клирингового центра не только по внутрироссийским операциям, но и по внешним операциям МПС, позволило бы оптимизировать технологические и финансовые издержки в сфере платежных карт в России.


Россия, потери, р.
5 000 000 000
4 500 000 000
4 000 000 000
3 500 000 000
3 000 000 000
2 500 000 000
2 000 000 000
1 500 000 000
1 000 000 000
500 000 000
0
2006
2007
2008
2009
2010
2011
2012
2013
2014

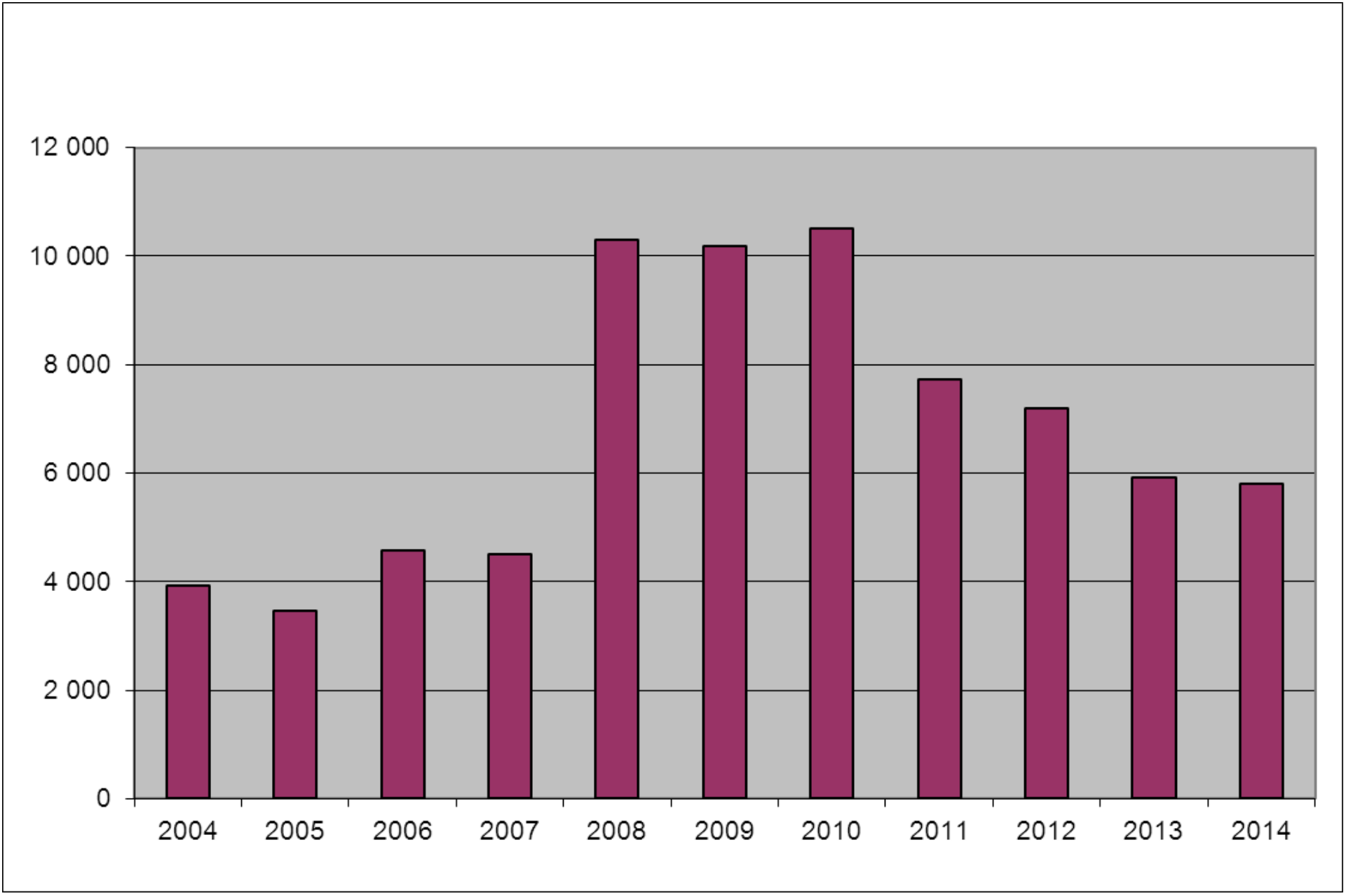
2014 г.

общие потери в РФ	3,7 млрд. рублей
эмиссионные потери	42%
эквайринговые потери	58%
банкоматы	27%
интернет	33%
подделки	36%
утраченные	17%

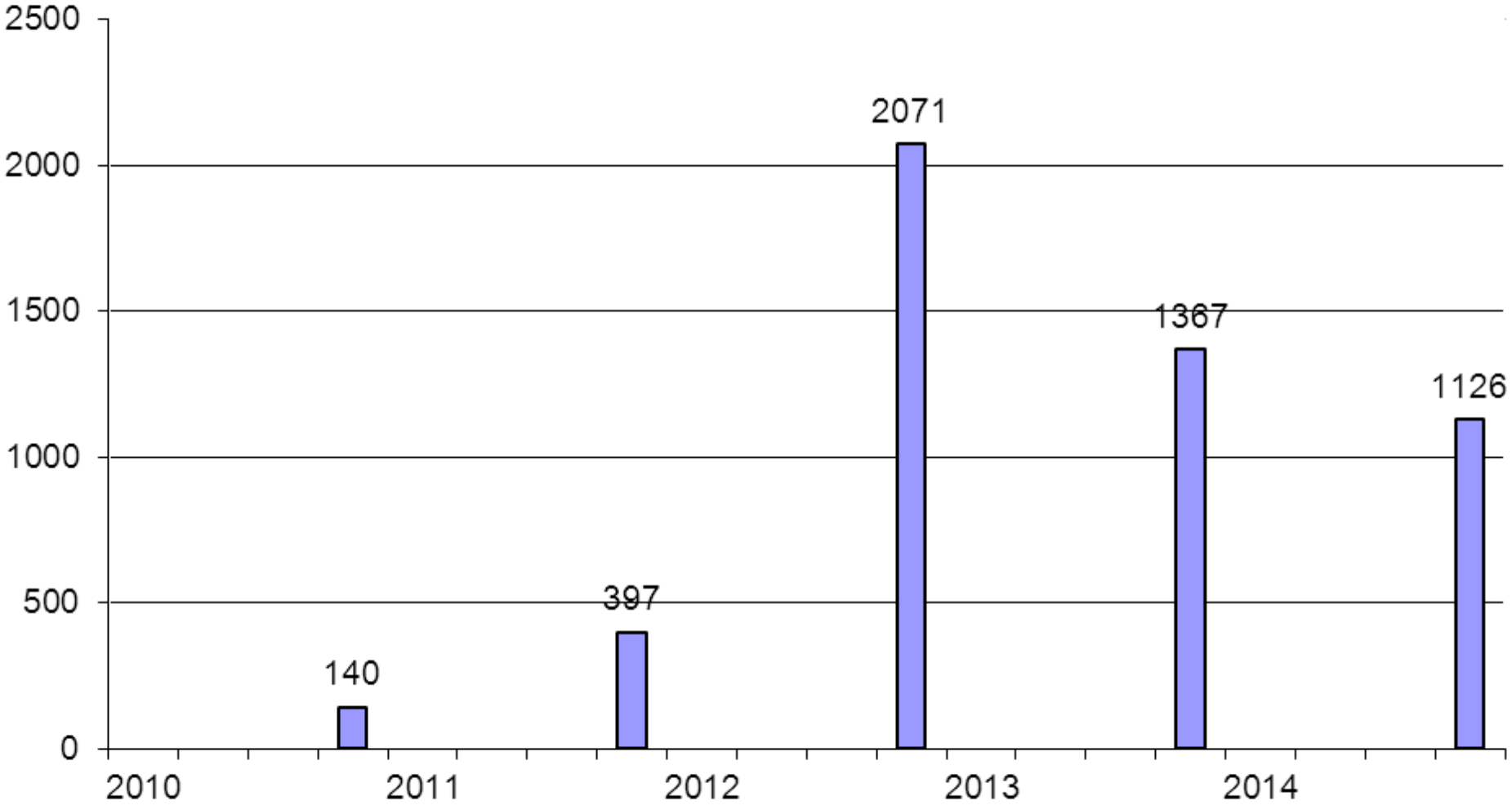
Относительные потери, bp

2014 г.	эмиссия	эквайринг
Россия	0,40	0,58
Мир	5,07	5,79

Скимминг, инциденты, Европа, EAST



Скимминг, инциденты, РФ, АУМ



Количество зарегистрированных УД

Статья УК РФ	**2013 год**	**2014 год**
159.3 Мошенничество с использованием платежных карт	1 297	925
159.6 Мошенничество в сфере компьютерной информации	693	993
187 Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов	4 000	309
272 Неправомерный доступ к компьютерной информации	1 799	1 150
273 Создание, использование и распространение вредоносных компьютерных программ	764	583
183 Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну	317	170

СПАСИБО!