Александр КРУПЧИК
директор
по развитию бизнеса
АО «ДиалогНаука»

О НЕОБХОДИМОСТИ PCI DSS

Сейчас, когда международная общественность ополчилась против российских банков, а ряд международных платёжных систем приостанавливают работу карт, выпущенных в России, встал важный вопрос о необходимости соответствия требованиям стандарта PCI DSS. Не достаточно ли просто соблюдения требований БР, которые предъявляются ко всем банковским информационным системам? В чём преимущества PCI DSS, чтобы российским банкам нужно было соблюдать его требования? Можно назвать целых три причины в пользу соблюдения требований PCI DSS, и в данной статье мы постараемся разобраться с ними.

ТРИ СЛОВА В ЗАЩИТУ PCI DSS

Первое: разные цели. Если сравнить требования БР и PCI DSS, то можно заметить, что цели у них разные. Требования БР направлены на обеспечение стабильного функционирования банковской системы России, а PCI DSS — разработан МПС для защиты конкретно от мошенничества с платёжными картами в организациях различных отраслей. Поэтому и подходы у этих стандартов разные. Требования БР направлены на построение риск-ориентированной защиты банковской системы страны от широкого спектра атак на информационные системы, в то время как требования PCI DSS основаны на оценке рисков, специфичных для индустрии платёжных карт, в том числе с учётом расследования реальных инцидентов.

В своё время МПС столкнулись со всё более увеличивающимися объёмами мошеннических транзакций, которые переросли в целую криминальную индустрию с оборотами в миллиарды долларов в год. PCI DSS возник для решения задач, связанных со снижением ущерба от мошенничества. Требования БР — это результат в большей части теоретической работы по систематизации защитных мер.

Требования PCI DSS основаны на оценке рисков, специфичных для индустрии платёжных карт, в том числе с учётом расследования реальных инцидентов

То, что требования по безопасности БР и PCI Council становятся более похожими друг на друга, является следствием того, что платёжные технологии с использованием платёжных карт и страновые финансовые системы имеют похожие карты рисков. Кроме того, имеет место повышение уровня зрелости отрасли информационной безопасности в целом, что предполагает более стандартизованные подходы в построении защиты информационных систем. Различные разрозненные «лучшие практики» трансформировались в систематизированные и достаточно стандартизованные архитектуры, структуры, технологии и процессы безопасности.

Второе: теория и практика. Требования БР — законодательные, а PCI DSS — практический стандарт. Банк России разработал свои требования в том виде, в котором ему было удобно, и сейчас они являются неотъемлемой частью законодательного регулирования. В то же время PCI DSS разработан «снизу» — он стал результатом договорённости нескольких платёжных систем по реализации ими мер защиты от мошенничества.

МПС работали в большом количестве стран мира, в том числе в странах, в которых государства никак не регулировали мероприятия по части информационной безопасности либо не уделяли внимания регулированию в области безопасности платёжных карт. Всё большее количество инцидентов и их масштабы начали подрывать доверие к использованию платёжных карт как средства платежа в целом. Каждая платёжная система начала разрабатывать различные требования и подходы к обеспечению безопасности данных платёжных карт. Требования разрабатывались в основном реактивно по результатам расследования различных инцидентов. Вначале требования не носили системного характера и отличались у каждой МПС. Проверку соответствия этим требованиям проводили сами платёжные системы. Компании, работающие с несколькими МПС, должны были проходить аудиты на соответствие у каждой из них по отдельности по разным требованиям, которые при этом могли противоречить друг другу.

Из-за этого возник запрос от участников платёжных систем на систематизацию и гармонизацию требований, а также сокращение количества аудитов. При этом МПС столкнулись с тем, что у них не было необходимых ресурсов для проведения аудитов безопасности. Таким образом, ведущие МПС решили объединиться и создать организацию, которая бы занималась вопросами безопасности в индустрии платёжных карт в интересах МПС. Был создан PCI SSC, который и разработал PCI DSS, а также ряд других стандартов в области безопасности платёжных карт. Были разработаны процедуры аудита, а также процедуры аккредитации аудиторов и контроля качества их работы. При разработке требований PCI DSS учитываются мнения всех заинтересованных сторон, а не только МПС. Любая организация может принять участие в обсуждении новых стандартов PCI DSS или новых технологий, направленных на безопасность. Именно поэтому PCI DSS основан на международном опыте.

Третье: международные системы. Следует отметить, что международное взаимодействие платёжных систем остаётся: в России продолжает работать китайская система UnionPay. Важно при таком международном сотрудничестве обеспечить высокий уровень безопасности платёжных транзакций и защиту от мошенничества. Конечно, это можно сделать с помощью двустороннего договора, однако для защиты российской платёжной системы будет лучше, если её защита будет выполняться по единым и понятным для всех правилам. Собственно, в своё время к PCI SSC присоединились UnionPay и НСПК, которые теперь требуют соответствия стандарту PCI DSS от участников своих платёжных систем.

В России требования безопасности определяет НСПК (как оператор платёжной системы «МИР»). Аналогично упомянутым ранее МПС, НСПК не является регулятором для российских банков. Но НСПК определяет требования ИБ в рамках договорных отношений с участниками платёжной системы.

Организации, работающие с картами «МИР», могут являться и нерезидентами РФ, и в этом случае на них не могут распространяться требования российских регуляторов. Но НСПК в рамках договорных требований может требовать от них соответствия PCI DSS в рамках общепринятых подходов и механизмов, имеющихся в индустрии платёжных карт. Если НСПК откажется от PCI DSS, то нужно будет разрабатывать собственный стандарт безопасности, а это затруднит распространение «МИР» в других странах — кому захочется выполнять специфические требования по безопасности.

К тому же кризис — не навсегда. Остальные МПС, возможно, вернутся в той или иной мере.

Если НСПК откажется от PCI DSS, то нужно будет разрабатывать собственный стандарт безопасности, а это затруднит распространение «МИР» в других странах — кому захочется выполнять специфические требования по безопасности

С НАДЕЖДОЙ НА БУДУЩЕЕ

Если подытожить всё вышесказанное, то можно сделать вывод, что требования стандарта PCI DSS необходимо соблюдать — этого требуют НСПК и UnionPay. Если же говорить о подходах к аккредитации аудиторов по стандарту PCI DSS, то здесь возможны следующие варианты.

- БР создаёт свою систему аккредитации аудиторов, которые проводят аудиты на соответствие требованиям БР. Они должны полностью перекрывать требования PCI DSS. Отчёты отправляются в БР или уполномоченную им организацию. Минусом является то, что необходимо договориться со всеми МПС, что результаты таких аудитов будут ими признаваться. Этот минус можно устранить на законодательном уровне, издав закон, который обязует МПС, работающие на территории РФ, признавать результаты таких аудитов.
- БР признаёт аккредитацию аудиторов, которую осуществляет PCI SSC. При этом аудиторы проводят аудиты на соответствие требованиям БР, которые полностью перекрывают требования PCI DSS. Банк проходит один аудит, в рамках которого проверяется соответствие сразу всем стандартам, по результатам аудита составляется отчёт для БР, а также AOC и ROC, направляемые в МПС. Основным минусом является то, что чувствительные данные об организации безопасности нашей платёжной инфраструктуры передаются в МПС враждебных государств (в основном Visa). Этот минус можно устранить распоряжением БР, в котором нужно указать, что за границу могут передаваться только отчёты о результатах аудита, которые содержат деперсонализированные данные, с указанием того, какие данные и каким образом должны быть деперсонализированы и как аудитор должен хранить у себя записи, на основании которых в случае необходимости можно будет сопоставить деперсонализированные и реальные данные, собранные во время аудита. В таком случае реальные данные останутся у аудитора и могут передаваться в сторонние организации только в рамках расследования крупных инцидентов.