

Требования PCI DSS и Закона «О персональных данных». Что общего?



Максим Эмм

Директор
департамента аудита
компания
«Информзащита»

В 2010 г. ожидается реализация нескольких крупных инициатив в части защиты данных. Во-первых, к 1 января 2010 г. должны были быть выполнены все требования законодательства о защите персональных данных в Российской Федерации, а во-вторых, в 2010 г. (последний срок — сентябрь 2010 г.) должны быть выполнены все требования стандарта PCI DSS.

Что же еще есть общего между этими требованиями индустрии платежных карточек и требованиями по защите персональных данных?

В первую очередь, и то, и другое нацелено на снижение рисков информационной безопасности, реализация которых наносит ущерб какой-то третьей стороне. В случае PCI DSS ущерб может быть нанесен банкам, выпустившим пластиковые карточки, и их клиентам, а в случае нарушений Закона о защите персональных данных — непосредственно населению.

Второе — это обязательность выполнения. Нельзя (во всяком случае, долго) обрабатывать данные платежных карточек или персональные данные граждан и не думать об их защите в соответствии с условиями опубликованного стандарта, За-

кона и подзаконных актов. В этом отличие данных документов, например, от стандарта Банка России по обеспечению информационной безопасности банковской отрасли, который до сих пор для коммерческих банков носит чисто рекомендательный характер. Но тут нужно учитывать реалии — регуляторы не могут просто взять и начать всех штрафовать с определенной даты — негативные последствия в этом случае могут превысить положительный эффект от повышения уровня защищенности данных. На мой взгляд, регуляторы будут ужесточать свои требования постепенно, а не одновременно.

Третье — в требованиях индустрии платежных карточек и требованиях по защите персональных данных схож подход к классификации информационных систем по уровню риска. Для персональных данных риск увеличивается, если в системе происходит обработка более «чувствительных» данных (категории от 1-й до 4-й) и в большем объеме (больше 100 тыс. обрабатываемых субъектов, больше 1000 и меньше 1000). Информационным системам в зависимости от этого присваиваются классы (от K1 до K4).

БЕЗОПАСНОСТЬ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

Для стандарта PCI DSS принцип тот же — разработчики стандарта разделяют информационные системы торговых предприятий, принимающих пластиковые карточки к оплате, и информационные системы поставщиков услуг, которые помогают провести транзакции (туда входят и сами банки). Для каждого из видов информационных систем риск определяется в зависимости от количества прошедших через них транзакций в год. Например, платежная система Visa определила для себя такой рейтинг торговых предприятий по количеству транзакций: до 20 тыс. в год, от 20 тыс. до 1 млн, от 1 млн до 6 млн и свыше 6 млн транзакций. Таким предприятиям присваиваются различные уровни от 1-го до 4-го.

На этом сходство между приведенными нормативными актами заканчивается. В PCI DSS в зависимости от уровня риска усиливаются требования к глубине контроля соблюдения условий стандарта. Например, с какого-то момента необходимо привлекать внешнего аудитора для ежегодного проведения оценки выполнения требований, при этом сами требования по защите информации одинаковы для всех категорий. В случае Закона о защите персональных данных требования по защите персональной информации растут с увеличением категории, к которой отнесены те или иные информационные системы, в то время как требования по глубине их контроля вообще пока не сформулированы. В настоящий момент только разрабатывается методика проведения контрольных проверок.

Еще одним существенным различием является способ контроля со стороны регулятора выполнения требований стандарта и Закона:

- для PCI DSS создан Совет, включающий в себя членов всех пяти платежных систем, признавших стандарт. Совет организует обучение и сертификацию аудиторов, которые потом проводят ежегодные проверки и консультируют предприятия по вопросам выполнения требований;
- Закон о защите персональных данных определяет три регулирующих органа — Роскомнадзор, ФСТЭК и ФСБ, каждый из которых отвечает за контроль выполнения «своей» части требований.

Кроме того, различаются области применения требований PCI DSS и Закона о защите персональных данных:

- Требования PCI DSS нацелены на защиту в первую очередь таких данных, как номер карточки (PAN), имя и фамилия держателя карточки (если они хранятся вместе с номером карточки), содержимое магнитной полосы карточки (TRACK2) и другая сугубо техническая информация, необходимая для проведения транзакций.
- Требования по защите персональных данных адресованы в основном к бэк-офисным системам, как для основной АБС, так и для выпуска карточек и обслуживания клиентов. Именно в этих подсистемах хранятся персональные данные клиентов банка. Только в небольшой части из них есть данные платежных карточек, и то к авторизации платежей отношение не имеющие. При этом основными данными, подлежащими защите, являются ФИО, паспортные данные, адреса клиентов банка,

которые собирается при заключении договора на обслуживание.

В настоящей статье хотелось бы попытаться дать ответы на вопрос, связанный с защитой информации, который чаще всего волнует руководителей компаний: какие способы оптимизации затрат на соответствие стандарту PCI и Закону о защите персональных данных существуют сегодня?

Основной способ, подходящий для обоих случаев, — минимизация расходов и усилий на обработку и хранение защищаемых данных. Руководство организации должно пересмотреть существующие бизнес-процессы и системы их автоматизации, чтобы получить ответы на такие вопросы, как: на самом ли деле нужны указанные данные в этой системе? Можно ли их чем-нибудь заменить?

Как показывает опыт, часто в качестве, например, идентификатора клиента используется номер его пластиковой карточки, а ведь можно использовать любую уникальную последовательность цифр. Этот способ является наиболее предпочтительным, поскольку позволяет вообще уйти от необходимости выполнять требования регулятора по технической защите данных ввиду их отсутствия.

Еще один эффективный способ оптимизации затрат на обработку и защиту персональных данных — изоляция систем обработки персональных данных и/или данных платежных карточек от остальных информационных систем банка за счет использования межсетевых экранов, терминальных серверов и применения защитных мер только на этих изолированных системах. Такой подход не противоречит требованиям нормативных документов, но ограничивает область их применения.

Можно также разделить базу клиентских данных на две части. В одной части будет содержаться ФИО, а в другой — все остальные данные, при этом связь между ними будет осуществляться через отвлеченный уникальный идентификатор. В этом случае можно изолировать каждую из подсистем и понизить класс их защиты с K1 или K2 до K3 или даже K4, что существенно снизит затраты на обеспечение безопасности. Правда, такая доработка информационной системы может быть сама по себе довольно затратной, для каждого случая нужно считать затраты и выгоды.

Ну и последний (в рамках данного материала) способ — передать вопросы создания системы защиты персональных данных для соответствия требованиям Закона № 152-ФЗ и/или стандарта PCI DSS опытному консультанту. Это позволит избежать дополнительных затрат на реализацию необходимой системы «методом проб и ошибок» и значительно сократить сроки проекта.

Что же касается рекомендованного Банком России стандарта по ИБ для банков, то его реализация в значительной степени пересекается с выполнением требований PCI DSS: похожий набор процессов управления информационной безопасностью, частично совпадающий набор технических требований по защите. Мы в компании «Информзащита» с нетерпением будем ждать развития этой инициативы. 