СМУТНЫЙ СТАНДАРТ

БЕЗ ЭФФЕКТИВНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕГОДНЯ НЕВОЗМОЖНА ДЕЯТЕЛЬНОСТЬ НИ ОДНОЙ КРУПНОЙ КОМПАНИИ. В БАНКОВСКОМ СЕКТОРЕ РЕШЕНИЕ ЭТОЙ ПРОБЛЕМЫ ВИДИТСЯ ВО ВНЕДРЕНИИ СТАНДАРТА ЦБ, ПОЗВОЛЯЮЩЕГО ОБЕЗОПАСИТЬ БАНКИ ОТ УТЕЧЕК КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ. НА СЕГОДНЯ СТАНДАРТ ВНЕДРЕН ЛИШЬ В 5% РОССИЙСКИХ БАНКОВ, НО ПО ПРОГНОЗАМ СПЕЦИАЛИСТОВ, В БЛИЖАЙШИЕ ТРИ ГОДА ЭТО ЧИСЛО ВЫРАСТЕТ ДО 80%. АРТЕМ КУЛАКОВ

ДОБРОВОЛЬНО-ПРИНУДИТЕЛЬНЫЙ ПОРЯДОК Действующий сегодня стандарт Центробанка по информационной безопасности был введен 26 января 2006 года как обновленная версия его же 2004 года выпуска. В этом документе содержатся основные положения международных стандартов IT-безопасности и дается прямая инструкция по управлению операционными рисками и предотвращению утечек информации. Внедрение этого стандарта может обеспечить банкам соответствие положениям Базельского соглашения по капиталу Basel II (к которому Россия планирует присоединиться уже в 2009 году), а следовательно,— соответствие реалиям мирового финансового рынка. Важным аргументом в пользу стандарта эксперты считают и маркетинговый аспект: отвечая требованиям ЦБ, он служит своего рода гарантией защищенности и надежности банка, а значит, позволяет привлечь новых клиентов.

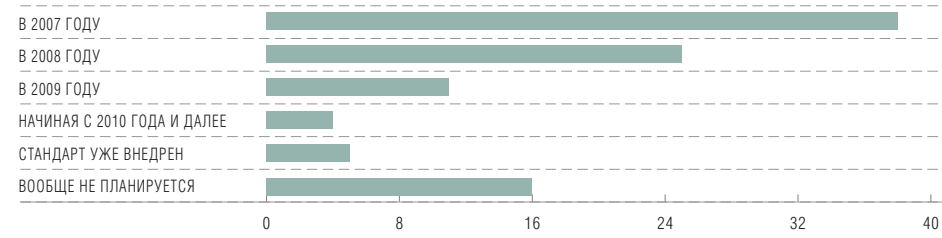
Официально стандарт Банка России носит чисто рекомендательный характер, то есть не является обязательным для введения. Тем не менее, как показало исследование «Стандарт Центробанка по IT-безопасности 2006», проведенное аналитическим центром InfoWatch совместно с порталом «Банкир.ру», большинство российских банков (72%) уверено, что в ближайшие три года его внедрение станет для них «обязаловкой».

Связано это в первую очередь с тем, что стандарт прямо или косвенно требует от банков создания систем защиты от утечек конфиденциальной информации. Дело в том, что в России, в отличие от США и стран Европы, до сих пор нет ни одного нормативного акта, который бы обязывал банк оповещать граждан в случае потери их персональных данных. Пользуясь этим, руководство компаний может просто сокрыть факт утечки и от правоохранительных органов, и от прессы, и даже от пострадавших. В противном случае репутации банка будет нанесен серьезный урон. «Когда об инциденте становится известно, портится имидж банка. Это, в свою очередь, приводит к потере лояльных клиентов и трудностям в привлечении новых. В результате снижается конкурентоспособность организации. Так что лучше предотвратить утечку, чем потом страдать от ее последствий»,— комментирует Денис Зенкин, директор по маркетингу компании InfoWatch.

АЛЕКСЕЙ КУДЕНКО

С ЯНВАРЯ 2006 ГОДА СТАНДАРТ БАНКА РОССИИ ВВЕЛИ ЛИШЬ 5% КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Известно, что угрозы IT-безопасности компании могут быть как внешними, так и внутренними. Долгое время бизнес в целом и банки в частности игнорировали внутренние риски, концентрируя внимание только на хакерских атаках, вредоносных кодах и спаме. Однако сейчас ситуация в корне изменилась: банкиры осознали, что инсайдерская утечка гораздо более опасна и менее контролируема. Согласно исследованию «Внутренние IT-угрозы в российском банковском секторе 2006», в ходе которого аналитический центр InfoWatch опросил более 300 отечественных кредитно-финансовых организаций, внутренние угрозы превалируют над внешними в соотношении шесть к четырем. В этом смысле введение стандарта ЦБ будет иметь двойной эффект — позволит не только повысить ответственность банка перед клиентами, но и защитить его от внутренних рисков.

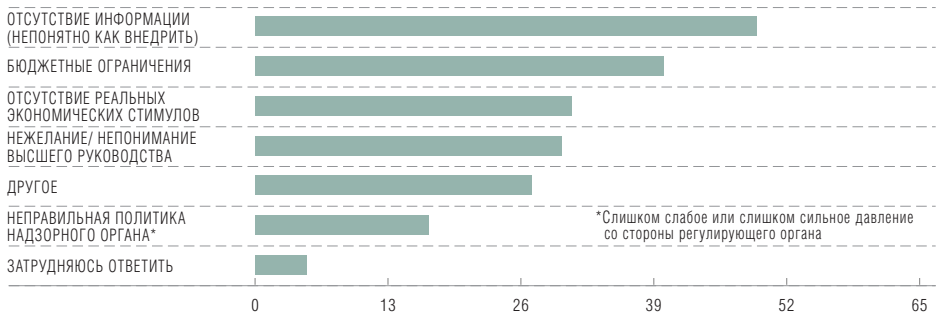


ПЛАНЫ ВНЕДРЕНИЯ СТАНДАРТА ЦБ ПО ИБ-БЕЗОПАСНОСТИ (%) ИСТОЧНИК: INFOWATCH, ABISS.

5% ВНЕ ОПАСНОСТИ На сегодняшний день стандарт Банка России введен лишь в 5% кредитно-финансовых организаций. Однако по результатам недавнего исследования «Стандарт ЦБ по IT-безопасности: внедрять или не внедрять?», в котором принял участие 101 российский банк, в 2007–2009 годах к ним планируют присоединиться еще 74%.

Между тем 16% опрошенных заявили о том, что не собираются участвовать в процессе еще как минимум два года. Представитель одного из таких банков объяснил это решение ожиданием результатов парламентских и президентских выборов, после которых ситуация в российском банковском секторе может резко измениться.

Как показало то же исследование, процесс внедрения стандарта по IT-безопасности тормозят сразу несколько факторов. Во-первых, около 50% российских банков до сих пор весьма смутно представляют себе, в чем суть этого документа и что им даст его принятие. Поскольку опыт тех мизерных 5% коллег едва ли можно считать наглядным примером, Центробанку следовало бы разработать пакет документов, детально разъясняющих всю методологию процедуры. Остальная часть опрошенных объяснила свое нежелание вводить стандарт большими материальными издержками (40%), отсутствием реальных экономических стимулов (31%), незаинтересованностью высшего руководства (30%) и неправильной политикой надзорного органа (17%). ■



ПРЕПЯТСТВИЯ НА ПУТИ ВНЕДРЕНИЯ СТАНДАРТА (%) ИСТОЧНИК: INFOWATCH, ABISS.

ВТОРОЕ БАЗЕЛЬСКОЕ СОГЛАШЕНИЕ (BASEL II)

Соглашение Basel II («Международная конвергенция принципов измерения капитала и стандартов капитала») было разработано и предложено Базельским комитетом по банковскому надзору и регулированию в 2001 году. Основная цель документа — выработать единый подход к управлению рисками финансовых организаций в международном масштабе. Положения Basel II уже применяются в ряде стран (ЕС, США, Япония, Индия), а Россия планирует присоединиться к договору в 2009 году. Однако учитывая жесткость требований, предъявляемых Базельским соглашением к финансовым организациям, через два года отвечать им в полной мере смогут только 15 крупнейших российских банков, остальным же придется приложить массу усилий для быстрой адаптации к новым реалиям.

В первую очередь Basel II требует подсчитывать резервируемый капитал на уровне центральной функции организации, а не отдельной бизнес-единицы. Другими словами, банк должен проанализировать информацию со всех подразделений, собрав ее в единой базе данных, что приводит к необходимости существенных инвестиций в IT-инфраструктуру. Более того, Basel II предписывает банкам выделять капитал для покрытия трех основных типов рисков — не только кредитных и рыночных, но и операционных. Между тем, как показало исследование «Соглашение Basel II в России 2006», в ходе которого аналитический центр InfoWatch и «Национальный банковский журнал» опросили 34 российских банка, именно операционные риски представляют основную проблему для отечественных кредитных организаций. 50% всех банков вообще не управляют ими, а другие 50% управляют лишь частично, а значит, неэффективно.

Под операционным риском Basel II понимает «риск убытка в результате неадекватных или ошибочных внутренних процессов, действий сотрудников и систем или внешних событий». Таким образом, именно в эту категорию попадают угрозы IT-безопасности, причем, как показало исследование «Соглашение Basel II в России 2006», для российских банков наибольшую угрозу представляют именно внутренние риски, в первую очередь неадекватные или ошибочные действия персонала. Выходов из сложившейся ситуации может быть несколько. Во-первых, «богатые» банки могут не внедрять ничего нового, а просто выделить серьезный капитал для покрытия инсайдерских рисков. Однако такой вариант потребует больших материальных затрат, поэтому вряд ли будет востребован. Во-вторых, банки могут свести к минимуму инсайдерские риски с помощью административных мер, серьезно ограничив доступ собственных сотрудников к конфиденциальным данным. Такой подход теоретически возможен, но на практике малоприменим, так как приведет к снижению эффективности работы банка в целом. Наконец, третий и наиболее разумный вариант предполагает внедрение специализированных систем, которое позволит взять под контроль львиную долю операционных рисков и уменьшить резервируемый капитал.