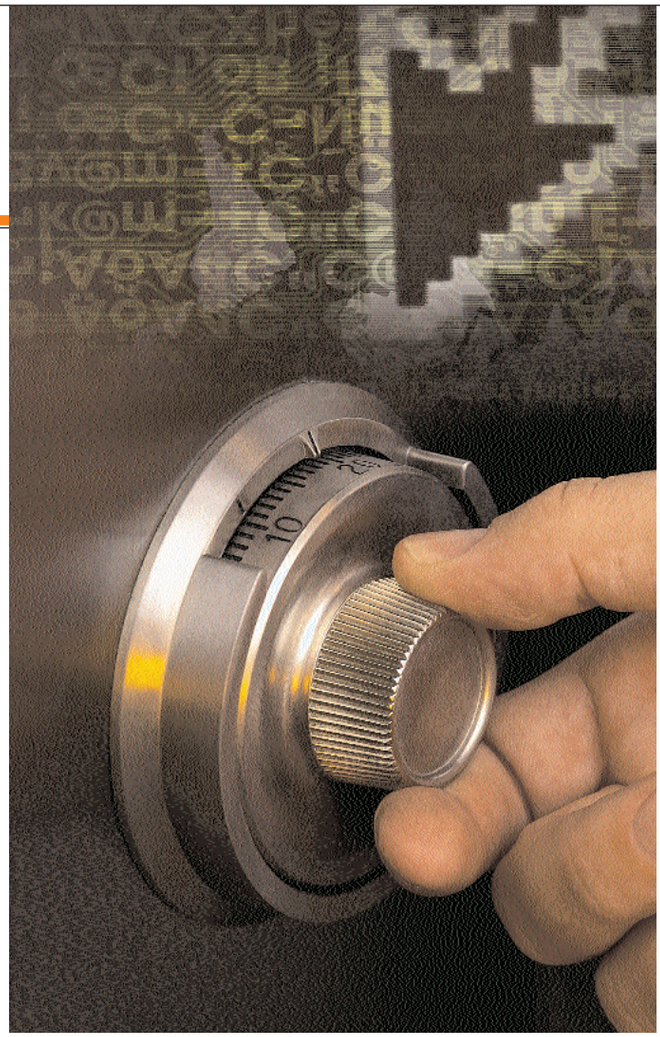
Владимир ПЕРМИНОВ,
начальник отдела консалтинга и поддержки продаж системно-аналитического департамента ЗАО «РНТ»

КАК НИ КИНЬ, АЛГОРИТМ ОДИН

МОДЕРНИЗАЦИЮ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКИ И КОМПАНИИ-КОНСУЛЬТАНТЫ ПРОВОДЯТ ПО ЕДИНОМУ СЦЕНАРИЮ



Перед руководством каждого банка рано или поздно встаёт вопрос о принятии и выполнении требований отраслевого стандарта информационной безопасности. Именно тогда приходится решать, пригласить профессионалов – поставщиков решений в лице аудиторов, консультантов и интеграторов или же постараться обойтись собственными силами. Что же проще и дешевле: озадачить собственных сотрудников, выбрать стороннего исполнителя, который всё наладит «под ключ», или же сочетать собственные усилия с помощью специализированных компаний?

ПЛАНУ ПРЕДШЕСТВУЕТ АНАЛИЗ

Чтобы добиться выполнения банком требований стандарта информационной безопасности Банка России, придётся выполнять один и тот же необходимый алгоритм независимо от выбора любого из перечисленных вариантов. Неизбежное начало – анализ текущей ситуации в банке, степени соответствия отраслевому стандарту, оценка того, что предстоит сделать, чтобы достигнуть требуемого уровня.

Такую предварительную работу должна провести специально сформированная рабочая группа, в состав которой входят: руководители служб IT, безопасности, риск-менеджмента, внутреннего контроля, организации банковских процессов, работы с персоналом. Возглавлять такую рабочую группу должен, конечно, представитель топ-менеджмента, уполномоченный принимать ответственные решения, распоряжаться финансами и прочими ресурсами.

Направлениями оценки служат техническое обеспечение и менеджмент, но главное – степень осознания руководством банка серьёзности задачи принятия и выполнения отраслевого стандарта информационной безопасности. Оценив степень несоответствия системы информационной безопасности банка стандарту Банка России, рабочая группа разрабатывает детальный план его выполнения.

В настоящее время наблюдается рост популярности среди банков темы информационной безопасности и соответствия стандартам информационной безопасности Банка России. «Толчком» стали сроки вступления в силу ФЗ-152 – закона о персональных данных. Сроки в очередной раз перенесли на год, но процесс, как говорится, пошёл. Защита персональных данных – лишь один, конъюнктурный аспект информационной безопасности кредитно-финансовых учреждений, решение которого потянет за собой остальные.

Защита персональных данных ? лишь один, конъюнктурный аспект информационной безопасности кредитно-финансовых учреждений, решение которого потянет за собой остальные

СФЕРА ОТВЕТСТВЕННОСТИ

В связи с перенесением сроков вступления в силу федерального закона о персональных данных именно этот аспект информационной безопасности банков продолжает оставаться наиболее актуальным. Поэтому первым делом следует классифицировать банковские информационные системы, обрабатывающие персональные данные: какие из них относятся к информационным системам персональных данных, и, соответственно, нуждаются в средствах защиты информации, прошедших процедуру оценки соответствия, а для каких достаточно применение уже разрешенных к использованию в банке средств защиты. Акты классификация составляются на основе требований и ре-

комендаций стандарта Банка России, которые разъясняют банкам отраслевую специфику применения требований ФЗ-152, облегчая их выполнение.

Следующий объект внимания рабочей группы – определение сферы ответственности системы управления информационной безопасностью банка, в частности – разграничение с задачами обеспечения общей безопасности. Из богатого перечня банковских функций вычленяется перечень ключевых бизнес-процессов, информационная защита обслуживания которых автоматизированной банковской системой необходима не для «галочки». Такие, например, как дистанционное банковское обслуживание, ряд фрагментов системы электронного документооборота, формирование отчетности. Идентифицируются задействованные в них ресурсы – техника, программное обеспечение, данные, площадки и персонал.

Совершенствование системы менеджмента информационной безопасности ведётся на основе оценки рисков для избранного перечня бизнес-процессов. Информационные банковские риски ранжируются по степени их значимости (высокие, средние и низкие), исходя как из степени возможного ущерба, так и из его вероятности. Выбираются риски, которые подлежат снижению до приемлемого уровня. Критерий отбора – соотнесение результатов с необходимыми затратами и имеющимися ресурсами. На случаи актуализации и реализации каждого вида рисков разрабатывается план реагирования – описание действий и их порядок.

ОТ ПРОЕКТА ДО ЗАПУСКА

На основании сделанного прописываются меры совершенствования банковской организационно-распорядительной документации, которая регламентирует менеджмент информационной безопасности. Главные из этих документов – официальная политика информационной безопасности и меры по совершенствованию её обеспечения, описание принципов управления документацией по информационной безопасности, процедуры управления инцидентами, а также регламенты управления рисками в этой сфере, проведения самооценки и т.д. Весь комплекс документов ранжируется по степени конфиденциальности и должен поддерживаться в последней, актуальной версии.

Внедрение разработанных мер предполагает распределение обязанностей между всеми участниками процесса, а также инструктаж всех сотрудников банка, а также, при необходимости, контрагентов и клиентов: корпоративных и индивидуальных.

Заключительный этап – модернизация собственно системы информационной безопасности банка. На основании

На случаи актуализации и реализации каждого вида рисков разрабатывается план реагирования ? описание действий и их порядок

Постепенно сотрудники и руководство банков приобретают способность оценить эффективность результата и самостоятельно поддерживать обеспечение информационной безопасности на заданном уровне

проведённого анализа и сделанных наработок последовательно разрабатываются техническое задание и технический проект. При необходимости проводится модернизация, обновление и докупка необходимого оборудования и средств защиты информации, на все задействованные устройства разрабатывается рабочая документация для пользователей и администраторов. Также возможно задействовать резервные мощности на случай форс-мажора – например, заключаться договоры с центрами обработки данных при соответствующих мерах обеспечения информационной безопасности.

Завершающий шаг – пусконаладочные работы.

В ОДИНОЧКУ ИЛИ ВМЕСТЕ

Когда принимать отраслевые стандарты информационной безопасности официальным «руководством к действию», решает руководство банка. Оно же задаёт темпы приведения собственной системы информационной безопасности в соответствие с требованиями стандарта Банка России. И выбирает, каким путём идти: попытаться обойтись собственными силами или привлечь специализированную компанию-консультанта, чтобы она провела модернизацию «под ключ», либо в качестве помощника.

Решая, привлекать специализированную компанию для полного выполнения объёма работ, либо фрагментов, нужно учитывать особенности обоих вариантов. В ходе совместной модернизации системы информационной безопасности в соответствии с отраслевыми стандартами сотрудники и руководство банков приобретают способность оценить эффективность результата и самостоятельно поддерживать обеспечение информационной безопасности на заданном уровне.

При проведении работ сторонним исполнителем «под ключ» для полной уверенности в успехе можно заказать аудит обновлённой системы обеспечения информационной безопасности банка у другой сторонней организации. Его итоги пригодятся также для представления в Банк России.

* * *

Практика показывает: в редком банке решение руководствоваться стандартом Банка России принимается без консультаций привлечённых специалистов. Путь ступенчатого повышения степени соответствия информационной безопасности отраслевым стандартам непрост. Банки, как правило, не решаются проходить его в одиночку, чаще привлекают организации-консультантов. Критерии выбора лучшей – это уже другая, отдельная тема.