УДК 004.05
ГРАНТИ 81.93.29

СТРАТЕГИЯ АДАПТАЦИИ КРЕДИТНЫХ ОРГАНИЗАЦИЙ К ИЗМЕНЕНИЯМ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

А.А. Лейфер
(Санкт-Петербург, Университет ИТМО)

Научный руководитель – к.т.н. А.С. Исаев
(Санкт-Петербург, Университет ИТМО)

Существует несколько взглядов на понимание термина «стратегия». В первом случае под стратегией понимается долгосрочный план достижения конкретной цели. Во втором – качественное направление развития, движение в рамках которого должно привести к достижению поставленной цели. В контексте обеспечения информационной безопасности разработка конкретного плана действий не всегда возможно ввиду быстрого изменения внешних факторов. В законодательство вносятся поправки, вычисления становятся дешевле, защита от вычислений – дороже. Таким образом, под стратегией адаптации кредитных организаций к изменениям законодательства в сфере защиты информации мы будем понимать скорее вектор развития, результат анализа внешних и внутренних факторов банка, нежели конкретный перечень действий.

Первый раздел стратегии должен содержать миссию и ценности кредитной организации в сфере защиты информации. «Надежный» и «безопасный» - именно таким клиенты хотят видеть банк, которому доверяют свои средства, поэтому безопасность обслуживания должна быть одной из основных ценностей в банке. Цели и задачи должны вытекать из миссии и содержать основные направления соответствия законодательству, а именно:

— соблюдение банковской тайны;
— безопасность переводов денежных средств;
— противодействие неправомерному использованию инсайдерской информации и манипулированию рынком;
— противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
— защита персональных данных;
— безопасность дистанционного банковского обслуживания;
— осуществление операций с применением систем Интернет-банкинга;
— безопасное использование банковских карт.

Определение заинтересованных сторон, затрагивающих процессы обеспечения соответствия законодательства, необходимо для валидации положений стратегии. Можно выделить широкий перечень заинтересованных сторон: регулирующие органы, топ-менеджмент банка, руководство подразделений информационной безопасности и комплаенса, бизнес-подразделения, ИТ-подразделения, юристы и др. При работе с заинтересованными лицами необходимо выделять их интересы, оценку влияния и стратегию для обеспечения поддержки.

Стратегия должна устанавливать виды информации, защищаемой в банке. Четко обозначить виды защищаемой информации важно ввиду того, что для них устанавливаются разные требования к защите. Также для всех видов защищаемой информации должна быть установлена взаимосвязь с направлениями защиты информации в банке и бизнес-процессами, ориентированными на безопасность.

Стратегия должна устанавливать ресурсы, необходимые для достижения заявленной цели. Ресурсы могут быть материальными (аппаратные и физические средства защиты

информации) и интеллектуальными (технологии защиты информации, интеллектуальная собственность, человеческий капитал). На этапе разработке стратегии желательно привлекать сотрудников, которые в дальнейшем будут реализовывать положения стратегии на практике. В качестве таких сотрудников могут выступать системные инженеры, разработчики мобильных приложений, Интернет-банков, владельцы продуктов и другие сотрудники, создающие интерфейсы между сотрудниками банка, клиентами и банковскими системами. Затраты на трудовые ресурсы могут быть подсчитаны исходя из оценки продолжительности работ и почасовых ставок сотрудников.

Среди качественных характеристик стратегии можно выделить следующие:

1) Полнота. Содержание стратегии должно быть необходимым и достаточным для того, чтобы применять ее для адаптации к изменениям в законодательстве.

2) Целостность и непротиворечивости отдельных элементов. По ходу всей стратегии должна отслеживаться взаимосвязь миссии, целей, задач, бизнес-процессов, организационных и программно-аппаратных средствах защиты.

3) Практическая применимость. Стратегия адаптации банковскому законодательству в сфере защиты информации не должна быть оторвана от реальности.

4) Адекватность. Содержание стратегии должно соответствовать ситуации, целям функционирования организации, ее техническим и организационным возможностям.

Таким образом, разработка стратегии адаптации в современных реалиях должна балансировать между незрелыми законодательными актами, дорогими технологиями защиты и изощренными инструментами нарушителей информационной безопасности. Положения стратегии должны стать «дорожной картой», помогающей ориентироваться в запутанном мире защиты информации. Важно, чтобы происходило постоянное управление и актуализация положений стратегии. Достижение баланса при этом должно осуществляться путем анализа обратной связи между работой стратегии в прошлом и текущем моменте времени.