Титов А.С.

БГЭУ, ФФБД, группа ДФК-1, 2 курс

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАНКОВСКОЙ СИСТЕМЕ

Масштабный сбой в работе организаций, осуществляющих деятельность в банковском секторе, может привести к развитию системного кризиса всей платежной системы и, как следствие, к экономическому коллапсу в масштабе государства. Среди причин, способных вызвать подобный сбой, отдельной группой выделяются угрозы информационной безопасности организаций банковской системы. Данный вид угроз оказывает непосредственное влияние на операционный риск основной деятельности банка, а значит, сказывается на его бизнес-процессах [1]. От обеспечения безопасности информационной вычислительной системы банка сегодня во многом зависит бесперебойное, устойчивое и надежное функционирование бизнес-процессов, в частности репутация финансового учреждения, доля на рынке, снижение издержек.

Сложность защиты информации в банковском секторе определяется не только огромными массивами обрабатываемых данных и изощренностью средств, применяемых злоумышленниками для доступа к ним. Она характеризуется еще и тем, что банки, являясь частью единой финансовой системы государства, должны соответствовать жестким требованиям безопасности, но реализацию этих требований государство полностью возложило на сами кредитные организации [1].

Таким образом, к нынешним автоматизированным банковским системам предъявляются строгие требования как со стороны банков-пользователей, так и со стороны государственных и контролирующих органов. Но с другой стороны, банковское обслуживание, в частности дистанционное, должно быть простым и удобным для клиента, иначе предлагаемая услуга не станет массовой и не принесет банку ту прибыль, ради которой она вводилась. Однако чем проще доступ к услуге, тем сложнее обеспечить безопасность данных и не допустить незаконных

транзакций. К тому же банковская система должна оставаться прозрачной для государственных надзорных и налоговых органов.

В целом ИТ-инфраструктура крупного универсального банка включает до нескольких сотен информационных систем, каждая из которых может стать слабым звеном с точки зрения безопасности. Риски в банковской сфере высоки, разнообразны и связаны не только с криминалом, но и с потерей информации и оперированием недостоверными данными в результате технических сбоев или влияния человеческого фактора.

Поэтому обеспечение информационной безопасности требует комплексного подхода, который включает правовые, организационные, технические, кадровые и другие аспекты, что связано с многогранностью задач, требующих решения. К созданию системы обеспечения информационной безопасности должны быть причастны не только служба информационной безопасности, ИТ-служба, но и топ-менеджмент, юридическая служба и другие структуры.

Поскольку обеспечение безопасности – это непрерывный процесс, то для него требуется непрерывный цикл мероприятий: планирование, реализация, проверка, действие. Следовательно, система менеджмента информационной безопасности должна стать частью общей системы менеджмента банка. А эффективными способами минимизации риска информационной безопасности – составление политики информационной безопасности банка (в том числе с учетом результатов анализа и оценки данного риска), а также последующая реализация и совершенствование системы менеджмента информационной безопасности банка в соответствии с этой политикой.

Литература

1. Шубин, А. Актуальные вопросы обеспечения информационной безопасности в банковской сфере / А. Шубин // Connect! Мир Связи [Электронный ресурс]. – 2008. – № 11. – Режим доступа: http://www.connect.ru/article.asp?id=9057. – Дата доступа: 17.04.2011.