УДК 004.056.5:336.71

ПОДХОДЫ К ЗАЩИТЕ БАНКОВСКОЙ ИНФОРМАЦИИ

Д.Ю. Тихонович, Н.Н. Трофимук, *3 курс*
*Научный руководитель – **Л.П. Володько**, к.э.н., доцент*
Полесский государственный университет

В то время как ежегодно во всем мире увеличивается зависимость различных организаций от использования информационных технологий (ИТ), возрастает и количество информации, подлежащей защите.

В связи с этим, можно утверждать, что на сегодняшний день защита информации является актуальным вопросом в любой сфере деятельности: производственной, торговой, образовании, стра-

ховании и др. Не является исключением и банковская сфера. Это вызвано рядом причин, среди которых существенным является тот факт, что банковская сфера представляет собой важную систему экономики, масштабный сбой в которой может привести к развитию кризиса всей платежной системы, и как следствие, к экономическому коллапсу в масштабе всего государства. Немало важным является обеспечение определенного «имиджа безопасности» банка для клиентов, то есть уверенность в том, что конфиденциальная информация не будет доступна посторонним людям. Обеспечение необходимого уровня информационной безопасности (ИБ) также позволяет повысить уровень надежности работы с информационными ресурсами.

В последнее время все большее число банков соглашается с необходимостью создания системы эффективного противодействия угрозам ИБ, которые оказывают непосредственное влияние на операционный риск основной деятельности банка, а значит, сказываются на его бизнес-процессах.

Для построения эффективной системы защиты информации необходимо провести следующие работы: определить угрозы безопасности информации, выявить возможные каналы утечки информации, выбрать соответствующие меры, методы и средства защиты.

Прежде чем говорить о разработке конкретных мероприятий, направленных на защиту информации, необходимо определить наиболее опасные угрозы безопасности. Согласно исследованию «Инсайдерские угрозы 2009» наиболее опасными угрозами являются: утечка информации (73%) и халатность персонала (70%), и лишь затем – вирусы, хакеры, кража оборудования, аппаратные и программные сбои [1]. Это говорит о том, что наибольшую опасность представляют собой внутренние угрозы, по сравнению с внешними. Среди наиболее опасных угроз внутренней безопасности были отмечены: утечка данных – 55%, искажение документации – 54%, кража оборудования – 25%, сбои в работе – 12% и др.

Важным также является выявление той информации, которая чаще всего подвергается утечке или уничтожению. По данным опроса, группу особого риска составляют персональные данные – 68%, что вызвано ростом обеспокоенности со стороны различного рода компаний. Утечке также подвергаются финансовые отчеты и детали конкретных сделок (41% и 40% соответственно).

Для обеспечения защиты информации существует ряд методов: организационные, аппаратные, программные, физические, морально-этические, законодательные. Совокупность мероприятий, входящих в состав каждой из группы методов, обладает как преимуществами, так и недостатками. В связи с этим весьма важно организовать процесс обеспечения ИБ таким образом, чтобы недостатки одних методов, компенсировались преимуществами других. Однако зачастую при обеспечении процесса информационной защиты на заднем плане остаются практически все методы, за исключением аппартно-программных, которым на сегодняшний день уделяется наибольшее внимание. Тем не менее, прежде чем внедрять и использовать широкий спектр аппаратных и программных разработок, на должном уровне развития должны находиться организационные методы.

Организационно-административные методы являются основой, базовым уровнем для всех последующих мероприятий. Неоспорим тот факт, что никакой другой уровень защиты не может эффективно работать без соответствующей административной поддержки.

Сегодня процесс обеспечение ИБ – комплексная задача, реализация которой важна для всех типов организаций, в частности – банков, где вопросам безопасности всегда уделяется повышенное внимание, как и ИТ в целом. Известно, что техническая составляющая в большинстве банков, как правило, находится на достаточно высоком уровне. Однако, что касается организационного уровня (то есть использования организационно-административных мероприятий), то он развит и организован в значительно меньшей степени. Внедрить организационные меры защиты означает, прежде всего, четко определить порядок доступа к соответствующим информационным системам: кто имеет доступ, к какой информации, на каких основаниях и т.п.; сертифицирование и стандартизирование защиты информации; определение должностных обязанностей сотрудников и др. На первый взгляд кажется, что выполнение вышеупомянутых действий не составляет особого труда. Однако в действительности это не так. Существенным фактором, сдерживающим развитие организационных методов ИБ, в частности организационно-административных, является отсутствие квалификации и опыта большинства специалистов, занятых в области обеспечения ИБ.

Важно отметить, что помимо создания новых систем обеспечения ИБ, усиленное внимание необходимо уделять поддержанию на должном уровне и совершенствованию уже существующих. Однако наблюдается сдержанность действий в данной области, что вызвано, прежде всего, бюджетными ограничениями – 46%, и лишь затем неэффективностью предлагаемых технологий – 35%, недостатком времени – 5% и юридическими барьерами – 2% [1].

Существенно сократить расходы на контроль за системой ИБ позволяет разработка политики информационной безопасности. Сравнение базовых принципов защиты организации и механизмов защиты способствует значительному росту надежности и эффективности. Наиболее эффективной схемой создания политики ИБ является последовательная разработка ее составляющих с привлечением специалистов различных областей.

На сегодняшний день, разработка концепции политики безопасности банка – один из наиболее эффективных способов, дополняющих комплекс мер, направленных на организацию ИБ. Преимущества данного документа заключаются в четкой и детальной последовательности описания глав и содержания политики, а также назначение ответственных в каждой области и регламентация деятельности сотрудников.

Можно сделать вывод о том, что защита банковской информации – важная задача, особенно в период роста и укрепления зависимости от ИТ. Ценным является грамотное сочетание всей совокупности существующих методов, основанных, прежде всего, на организационных мероприятиях. В связи с этим, деятельность любого банка, должна быть ориентирована на создание более высокого уровня защиты информационных ресурсов и ИТ- инфраструктуры, что в еще большей степени позволит повысить доверие клиентов и обеспечит стабильное, уверенное его функционирование и развитие.

Список использованных источников

1. Инсайдерские угрозы 2009 / Аналитический центр Perimetrix [Электронный ресурс]. – Режим доступа: http://www.perimetrix.ru/downloads/rp/PTX_Personal_Data_2009.pdf – Дата доступа: 22.12.2009 г.