

емлемым элементом механизма хищений денежных средств. В ходе подготовки и совершения хищений преступники добывают и используют информацию о счетах и вкладах клиентов банка, совершают неправомерный доступ к компьютерной информации, модифицируют банковские платежные технологические процессы, переводят деньги с чужих счетов на счета подставных лиц и т.д.

В то же время по-прежнему актуальными остаются задачи противодействия мошенникам на уровне традиционных технологий в сфере кредитования, использования аккредитивов, платежных поручений и векселей.

— С какой периодичностью банкам необходимо обновлять систему безопасности?

— Собственники банка и лица, ответственные за разработку и функционирование системы безопасности, должны четко осознавать, что система защиты интересов банка находится в непрерывной борьбе с теми, кто пытается незаконно завладеть его имуществом. Преступники непрерывно совершенствуют и обновляют средства и способы совершения преступлений. По этой причине система безопасности банка должна развиваться и совершенствоваться непрерывно с учетом средств и методов, разработанных современной наукой, рекомендаций по их наиболее эффектив-

ному применению, с использованием опыта борьбы с преступностью в банковской сфере отечественных и зарубежных правоохранительных структур, а также анализа собственного опыта.

В числе новейших средств защиты банковских услуг и операций, разработанных отечественной наукой, ряд наших банков с успехом использует аппаратные комплексы, реализующие возможности нанотехнологий, автоматического поиска информации о клиентах, оценки надежности клиентов и достоверности представленной ими информации, поддержки принятия решений и другие.

— Для обеспечения внутренней безопасности банки используют различные технологии: видеонаблюдение, ограничение доступа, контроллеры, биометрические технологии, охрану и т.д. Какие из них являются наиболее надежными? Какие предусмотрены регулятором, а какие банки внедряет по собственной инициативе?

— Система технических средств обеспечения безопасности банка включает в себя весьма широкий набор приспособлений. Однако в целом их можно разделить по функциональному назначению на четыре основных вида: технические средства охраны персонала, клиентов и имущества банка, технические средства защиты банковских операций и инструмен-

МНЕНИЕ ЭКСПЕРТА

Какими стандартами руководствуется банк при разработке системы безопасности?



Рустэм Хайретдинов

заместитель генерального
директора компании InfoWatch

Финансы — самая регулируемая в сфере защиты информации отрасль экономики. В информационной системе банка может находиться информация, составляющая банковскую и коммерческую тайну, персональные данные, а также другая информация, оборот которой регулируется.

С одной стороны, это создает трудности, так как информационной системе банка приходится одновременно соответствовать целому ряду регулирующих документов как российских, так и западных регуляторов.

С другой стороны, это и облегчает труд менеджмента, так как не надо ничего выдумывать, к требованиям прилагаются рекомендации по подготовке информационной системы к прохождению аудита на соответствие этим требованиям. Там четко написано — «делай это и это».

Проблема в этом случае не «что», а «как» делать, но для этого и существуют квалифицированные консультанты.

В первую очередь для соответствия банки выбирают обязательные требования, то есть те, нарушения которых влекут за собой административное или даже уголовное преследование. Это требования по защите банковской тайны и информации о платежных картах. Вскоре к ним добавятся требования по защите персональных данных, часть из которых обязательна уже сегодня.

Есть требования, решение о соответствии которым банк волен выбирать. У большого числа банков режим коммерческой тайны не введен, поэтому им не обязательно соответствовать требованиям ФЗ «О коммерческой тайне». А если банк не имеет филиалов в Европе, то требования соглашения Basel II для него тоже не обязательны.

Многие банки прошли или готовятся пройти аудит на соответствие Стандарту Банка России, хотя формально он не является обязательным. Это происходит потому, что разработчики Стандарта заложили в него требования, учитывающие большинство требований других стандартов. Соответствие ему ведет за собой соответствие требованиям многих других стандартов.

Соответствие требованиям регуляторов в последнее время является основной мотивацией при приобретении средств защиты информации как в России, так и за рубежом.