В.С. КУЗНЕЦОВ,
Национальный университет водного хозяйства и природопользования,
г. Ровно, Украина

ОСНОВНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ

Information safety of bank is a security of the information (a banking secrecy, secret of contributions, banking operations and so forth) from the non-authorized access, destruction, updating, disclosing to the third parties and delay at receipt.

В современных условиях глобализации нельзя в полной мере говорить об успешном развитии экономики без всестороннего и всеобъемлющего использования информационных технологий. Масштабное внедрение IT-технологий в кредитно-финансовую сферу может существенно повысить эффективность и качество работы всей банковской системы. В наши дни в связи с массовой информатизацией и компьютеризацией банковской сферы роль информационной безопасности банков значительно увеличилась. Одной из основных проблем, до сих пор сдерживающих развитие информационной безопасности банков в мире, является непонимание топ-менеджерами необходимости обеспечить не только физическую, но информационную безопасность банка.

С точки зрения зарубежных специалистов, преступный мир в недалеком будущем может отказаться от ограбления банков, так как незаконное использование компьютерных систем для совершения банковских операций дает больше прибыли при меньшем риске. Сегодня вопросы компьютерной или информационной безопасности банка становятся для ряда компаний не просто вопросами безопасности бизнеса, а еще и жизненной необходимостью дальнейшего развития. Действительно, со временем практически все банки будут предлагать клиентам схожий набор услуг при почти одинаковых условиях. В таком случае потенциальный клиент будет выбирать не по критериям "где процентные ставки по депозитам выше", или "кто предоставляет возможность мобильного управления счетом", а по критерию "какой банк надежнее защищен".

Сфера информационной безопасности – наиболее динамическая отрасль развития индустрии безопасности в целом. Сегодня около 90% всех преступлений связаны с использованием автоматизированных систем обработки информации банка (АСОИБ). Информационная безопасность постоянно требует новых инновационных идей и решений, так как телекоммуникационные и компьютерные технологии постоянно обновляются, и на компьютерные системы возлагается все большая ответственность. В свою очередь при создании, модернизации и обслуживании АСОИБ банкам необходимо уделять много внимания обеспечению ее безопасности. Практика показывает, что не существует сложных компьютерных систем, которые не содержали бы ошибок. В западных банках программное обеспечение разрабатывается конкретно под каждый банк, а особенности и устройства АСОИБ являются коммерческой тайной. В Украине в основном используются «стандартные» банковские программные продукты, информация о которых широко известна, что облегчает задачу несанкционированного доступа.

Основные изменения в банковской индустрии за последние десятилетия напрямую связаны с развитием информационных технологий. Наблюдается устойчивая тенденция к снижению оборота наличных денег и увеличению безналичных расчетов с использованием банковских платежных карт, глобальной сети Internet, терминалов управления счетами, устройств самообслуживания и, как следствие, рост числа преступлений как с использованием IT-технологий, так и с использованием служебного положения недобросовестными сотрудниками банков.

Факты говорят сами за себя. В марте 2003 года злоумышленники взломали несколько крупных американских серверов Visa и MasterCard. В руки хакеров попало несколько тысяч номеров кредиток с паролями, по которым они тут же сняли

довольно много наличных. В конечном итоге хулиганов поймали, а системы защиты Visa и MasterCard существенно переделаны, что значительно усложнило возможность их повторного взлома. Убытки банков и других финансовых организаций от вмешательства в их системы обработки информации составляют около 3 млрд. дол. США в год; размер убытков, связанных с использованием банковских платежных карт, оценивается в сумме 2 млрд. долл. США в год, что составляет 0,03-2% от общего объема платежей в зависимости от используемой системы. По данным Департамента по борьбе с экономической преступностью МВД Украины, за 9 месяцев 2006 года непосредственно в банках было совершено около 1200 преступлений, из которых более 80% признаны представляющими "повышенную общественную опасность". По словам представителей правоохранительных органов, большинство преступлений банкиров совершается в регионах. Это объясняется слабым контролем над деятельностью региональных банкиров как со стороны правоохранительных органов, так и со стороны топ-менеджмента банка. Также стоить упомянуть то, что банки и другие финансовые организации могут сознательно занижать или совсем не предавать огласке реальные суммы убытков от электронного мошенничества с целью предотвращения потери клиентов и ущерба своей репутации.

Целостную систему защиты создать достаточно сложно, так как существует много подходов и точек зрения на методологию ее построения. Сегодня речь идет о глобальной защите и ее отдельных аспектах: защита персональных компьютеров, сетей, баз данных и т.д. Как уже было сказано, нет абсолютно защищенных систем. С некоторой вероятностью можно говорить о надежности системы, а также о защите от определенной категории правонарушителей. Стратегия информационной безопасности банков существенно отличается от аналогичных стратегий других компаний и учреждений. Это обусловлено, прежде всего, специфическим характером угроз, а также публичной деятельностью банков, которые вынуждены делать доступ к счетам достаточно легким для удобства клиентов.

Информационная безопасность банка должна учитывать такие специфические факторы как:

- совокупность информации в банковских системах представляет собой реальные деньги, а с помощью компьютера ими можно оперировать;
- информация в банковских системах касается интересов большого количества людей и организаций – клиентов банка, и как правило, эта информация носит конфиденциальный характер, и банк несет ответственность за ее сбережение;
- конкурентоспособность банка зависит от удобства сотрудничества с ним, но простота доступа к деньгам увеличивает вероятность незаконного проникновения в банковскую систему;
- информационная безопасность банка должна обеспечивать высокую надежность работы компьютерных систем даже в случае внештатной ситуации, так как банк несет ответственность за деньги своих клиентов;
- обработка трансакций – это наиболее трудоемкий элемент технологического процесса банка, она должна быть безошибочной и обеспечивать точную и своевременную информацию.

В вопросах информационной защиты финансовых организаций главное – это оперативное и максимально полное восстановление информации после аварий и сбоев. Следующая по важности проблема – управление правами доступа пользователей к хранимой и обрабатываемой информации.

В завершение, хотелось бы выразить надежду, что руководители банковских организаций, начальники служб безопасности, осознанно будут относиться к решению комплексной проблемы защиты банка и используют для этого системный подход. При этом необходимо помнить, что теория, методы, способы и средства защиты должны развиваться и совершенствоваться, чтобы всегда быть на шаг впереди нарушителей и злоумышленников.

Защита – это своего рода игра обороны и нападения: кто больше знает и может предвидеть действенные методы, тот и выигрывает.