СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВ

Т.Ю. Журавлева
УО «Белорусский государственный экономический университет», Минск

Со времени своего появления банки неизменно вызывали преступный интерес. И этот интерес был связан не только с хранением в кредитных организациях денежных средств, но и с тем, что в банках сосредоточивается важная и зачастую секретная информация о финансовой и хозяйственной деятельности многих людей, компаний, организаций и даже целых государств.

В наши дни в связи со всеобщей информатизацией и компьютеризацией банковской деятельности значение информационной безопасности банков многократно возросло. В настоящее время свыше 90 % всех преступлений связано с использованием автоматизированных систем обработки информации банка.

Информационная безопасность банка должна учитывать следующие специфические факторы:

– хранимая и обрабатываемая в банковских системах информация представляет собой реальные деньги;

– обязательное сохранение конфиденциальной информации о клиентах банка;

– конкурентоспособность банка, то есть насколько клиенту удобно работать с банком и насколько широк спектр предоставляемых услуг;

– высокая надежность работы компьютерных систем даже в случае нештатных ситуаций.

Компьютерные преступления, как правило, затрагивают большое количество банковских операций (до нескольких сотен). Обычно злоумышленники используют собственные банковские счета, на которые переводят похищенные суммы.

В зарубежных финансовых системах главным в защите банков является оперативное, по возможности полное, восстановление информации после аварий и сбоев. В основном защита информации от разрушения достигается путем создания резервных копий и их внешнего хранения, использования средств бесперебойного электропитания.

Чаще всего при управлении доступом пользователей к хранимой и обрабатываемой банком информации используются приобретенные программные средства. Однако сертифицированные средства управления доступом составляют около 3 % от общего числа используемых программ. Это объясняется тем, что с сертифицированными программными средствами трудно работать и они дороги в эксплуатации.

К отличиям организации защиты сетей ЭВМ в банках можно отнести широкое использование стандартного (адаптированного, но не специально разработанного для конкретной организации) ПО управления доступом к сети, защиту точек подключения к системе через коммутируемые линии связи. Скорее всего это связано с большей распространенностью средств телекоммуникаций в финансовых сферах и желанием защититься от вмешательства извне. Другие способы защиты, такие как применение антивирусных средств, шифрование передаваемых данных (за исключением антивирусных средств) применяются менее чем половиной банков.

Большое внимание в финансовых организациях уделяется защите помещений, в которых расположены компьютеры, – охрана, кодовые замки и т.д. (около 40 % банков). Меньшее внимание уделяется защите телефонных линий связи и использованию ЭВМ, разработанных с учетом требования стандарта Tempest (защита от утечки информации по каналам электромагнитных излучений и наводок).

Анализ позволяет сделать важный вывод: защита банков строится несколько иначе, чем обычных коммерческих и государственных организаций. Следовательно, для защиты автоматизированных систем обработки информации банков нельзя применять те технические и организационные решения, которые были разработаны для стандартных ситуаций.

ЭКОНОМИКО-МАТЕМАТИЧЕСКАЯ МОДЕЛЬ МЕЖОТРАСЛЕВОГО БАЛАНСА

Е.А. Зайцева, О.С. Лашкова
Учреждение образования «Белорусский государственный экономический университет», Минск

Основой многих линейных моделей производства является схема межотраслевого баланса. Цель балансового анализа – ответить на вопрос, возникающий в макроэкономике и связанный с эффективностью