УДК 681.518

Раимбек уулу Э.– старший преподаватель ОшТУ

ОПТИМИЗАЦИЯ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМ И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВ

В данной статье рассматриваются банковские информационные системы, проблемы обеспечение информационной безопасности автоматизированных банковских систем (АБС) а также факторы для обеспечения информационной безопасности банков.

Ключевые слова и фразы: информационная безопасность; банковская система; автоматизированная банковская система.

Raimbek uulu E. – senior teacher OshTU

OPTIMIZATION OF AUTOMATED BANKING SYSTEM SECURITY AND PROVIDING INFORMATIONAL BANKING SYSTEM

This article examines banking information systems, problems of ensuring information security of automated banking systems (ABS), as well as factors for ensuring information security of banks.

Key words and phrases: information security, bank system; automated banking system.

Актуальность: *Банк являясь важнейшим финансовым институтом современного социума, должны следовать определенным правилам информационной безопасности и уметь противостоять дестабилизирующим факторам.*

Практическая значимость работы: В настоящее время стоимость и значимость банковской информации многократно возросли, что привело к росту преступного интереса к ней. Каждый банк обязан обеспечить безопасность хранимых им данных, именно поэтому он должен следить за регулярной сменой и проверкой паролей, а также за контролем вероятности утечки информации [2].

Банковские информационные системы и базы данных содержат конфиденциальную информацию о клиентах банка, состоянии их счетов и проведении различных финансовых операций. Необходимо поддерживать сохранность этих данных, обеспечивать их информационную безопасность, осуществлять быстрый и своевременный обмен и обработку информации, чтобы банковская система не дала сбой. Для этого необходима целая структура, которая будет способна обеспечить защиту информации, а также конфиденциальность клиентской базы.

Современные АБС – это сложные, структурированные, территориально распределенные сети. Как правило, они строятся на основе передовых технологий и программных средств, которые в силу своей универсальности не обладают достаточной защищенностью.

В то же время АБС становится одним из наиболее уязвимых мест во всей организации, притягивающим злоумышленников как извне, так и из числа сотрудников самого банка. Для подтверждения этого тезиса можно привести несколько фактов:

Потери банков и других финансовых организаций от воздействия на их системы обработки информации составляют около $ 3 млрд. в год.

Объем потерь, связанных с использованием пластиковых карточек, оценивается в $ 2 млрд. в год, что составляет 0,03-2% от общего объема платежей в зависимости от используемой системы.

Средняя величина ущерба от банковской кражи с применением электронных средств составляет около $ 9000.

Один из самых громких скандалов связан с попыткой семерых человек украсть $ 700 млн. в первом национальном банке, Чикаго. Она была предотвращена ФБР.

27 млн. фунтов стерлингов были украдены из Лондонского отделения Union Bank of Switzerland.

DM 5 млн. украдены из Chase Bank (Франкфурт). Служащий перевел деньги в банк Гонконга – они были взяты с большого количества счетов (атака «салями»). Кража оказалась успешной.

$ 3 млн. – банк Стокгольма. Кража была совершена с использованием привилегированного положения нескольких служащих в информационной системе банка и также оказалась успешной.

Чтобы обезопасить себя и своих клиентов, большинство банков предпринимают необходимые меры защиты, в числе которых защита АБС занимает не последнее место. При этом необходимо учитывать, что защита АБС – дорогостоящее и сложное мероприятие. Так, например, Barclays Bank тратит на защиту своей автоматизированной системы около $ 20 млн. ежегодно.

Datapro Information Services Group провела почтовый опрос среди случайно выбранных менеджеров информационных систем. Целью опроса явилось выяснение состояния дел в области защиты. Было получено 1153 анкеты, на основе которых получены приводимые ниже результаты:

- около 25% всех нарушений составляют стихийные бедствия;
- около половины систем испытывали внезапные перерывы электропитания или связи, причины которых носили искусственный характер;
- около 3% систем испытывали внешние нарушения (проникновение в систему организации);

70-75% – внутренние нарушения, из них:

– 10% совершены обиженными и недовольными служащими-пользователями АБС банка;

– 10% – совершены из корыстных побуждений персоналом системы;

– 50-55% – результат неумышленных ошибок персонала и/или пользователей системы в результате небрежности, халатности или некомпетентности.

Эти данные свидетельствуют о том, что чаще всего происходят не такие нарушения, как нападения хакеров или кража компьютеров с ценной информацией, а самые обыкновенные, проистекающие из повседневной деятельности. В то же время именно умышленные атаки на компьютерные системы приносят наибольший единовременный ущерб, а меры защиты о них наиболее сложны и дорогостоящи. В этой связи проблема оптимизации защиты АБС является наиболее актуальной в сфере информационной безопасности банков.

Материалы исследований: Факторы, которые следует учитывать для обеспечения информационной безопасности банков [3]:

1. Информация, которая хранится и обрабатывается в банках, – это реальные деньги. При открытом доступе к данной информации через компьютеры могут открываться кредиты, производиться выплаты, а также могут переводиться значительные суммы денег без ведома владельца данного счета. Совершенно ясно, что такое незаконное манипулирование информацией приведет к убыткам различной степени. Данная особенность увеличила число мошенников, которые покушаются именно на банки, ведь информация, к примеру, промышленных компаний чаще всего не представляет такого интереса.

2. Информация, которая относится к банковской сфере, касается большого количества людей и организаций, то есть клиентов банков. Банк должен обеспечить достаточный уровень конфиденциальности информации, что является приоритетной задачей, поскольку каждый клиент вправе рассчитывать, что банк будет заботиться о его интересах, ведь от этого напрямую зависят репутация и успешность самого банка.
3. От того, как клиенту удобно работать с банком, а также от широкого спектра предоставляемых им услуг напрямую зависит конкурентоспособность банка. Именно поэтому банк должен предоставлять возможность быстрого и неутомительного распоряжения денежными средствами. Но именно такая легкость доступа к денежным активам и увеличивает число преступников, которые проявляют интерес к банковским системам.
4. Банк обязан обеспечить высокую надежность работы компьютерных систем даже в случае нештатных ситуаций, ведь банк, в отличие от большинства компаний, отвечает не только за свои денежные средства, но и за деньги клиентов.
5. Банк хранит важную информацию о своих клиентах, что расширяет круг потенциальных злоумышленников, заинтересованных в краже или порче такой информации.

Основной вывод, который можно сделать из анализа развития банковской отрасли, заключается в том, что компьютеризация банковской деятельности продолжает возрастать. Основные изменения в банковской индустрии за последние десятилетия связаны именно с развитием информационных технологий. Можно прогнозировать дальнейшее снижение оборота наличных денег и постепенный уход на безналичные расчеты с использованием пластиковых карт, сети Internet и удаленных терминалов управления счетом юридических лиц.

Заключение:

В связи с этим следует ожидать дальнейшее динамичное развитие средств информационной безопасности банков, поскольку их значение постоянно возрастает.План действий, обеспечивающих информационную безопасность банков, принципиально отличается от плана действий других организаций. Главными причинами этого являются специфический характер угроз, а также публичная деятельность банков, которые обязаны делать доступ к счетам несложным с целью удобства для клиентов.

Литература:

1. **Ясенев, В.Н.** Информационная безопасность в экономических системах [Электронный ресурс]: учебное пособие. Н. Новгород: Изд-во ННГУ, 2006. URL: http://www.iee.unn.ru/files/posobya/ib_yasenev.pdf (дата обращения: 06.07.2015).
2. Особенности обеспечения информационной безопасности в банковской системе [Электронный ресурс].URL: http://www.antimalware.ru/analytics/technology_analysis /features information security in the banking system (дата обращения: 06.07.2015).
3. Проблемы информационной безопасности банков [Электронный ресурс]. URL: http://uchit.net/catalog/Bankovskoe delo/81596/ (дата обращения: 06.07.2015).