УДК 004.056.5

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОКОНЕЧНОГО БАНКОВСКОГО ОБОРУДОВАНИЯ

ГОНДАГ САЗ МОСТАФА МОХАММАД,
МОЗДУРАНИ ШИРАЗ МОХАММАД ГОЛАМХОССЕЙН

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
kafzi@bsuir.by

Рассмотрена проблема обеспечения безопасности современных терминалов самообслуживания, применяемых в банковским секторе.

Ключевые слова: банковский терминал, мошенничество.

Предложение банковских услуг через сеть терминалов самообслуживания становится массовым явлением. Как показывает мировая практика 90% банковских услуг, оказываемых в рамках традиционных отделений банка, может быть не только автоматизировано, но и переведено в сферу самообслуживания с помощью современных терминальных устройств.

Существующая система безналичных расчетов по розничным платежам на основе применения электронных платежных инструментов представлена в основном системами расчетов с использованием банковских пластиковых карточек и электронных денег.

В целях обеспечения безопасной и надежной деятельности при осуществлении операций с электронными деньгами банки должны соблюдать нормативы безопасного функционирования.

Под безопасностью системы банковских терминалов понимают их свойство, выражающееся в способности противодействовать попыткам нанесения ущерба владельцам и пользователям системы при различных (умышленных и неумышленных) воздействиях на нее. Следует отметить, что природа воздействия может быть самой различной, а следовательно и поле для угроз безопасности достаточно обширное.

Для многих банков характерно то, что нарушение безопасности информации в их конечных банковских терминалах может нанести огромный материальный ущерб, как самим банкам, так и их клиентам. Поэтому эти организации вынуждены особое внимание уделять гарантиям безопасности, что ведет к необходимости реализации комплексной защиты.

Комплексный подход к обеспечению безопасности, а так же постоянный мониторинг и поиск новых угроз являются ключевым моментом обеспечения безопасного функционирования конечных банковских терминалов.

Физическое воздействие на конечный банковский терминал - один из первоочередных вопросов. Защита от вандализма, погодных условий, попытки физического взлома – решаются путем совершенствования конструкции терминалов: установкой сейфов с различными видами замков (с двойной комбинацией, с двойной комбинацией и дистанционным доступом и др.); доработкой кассет и контейнеров загрузки, хранения банкнот, исключающих доступ к денежным средствам; установкой различного рода тревожных датчиков (датчики тревожной сигнализации, сейсмические датчики, датчик температуры и др.); установкой источника бесперебойного электропитания; установкой встроенной камеры видеонаблюдения, а так же тщательным исследованием места установки терминала с точки зрения безопасности его использования.

Внешний вид терминала, а так же расположение его основных функциональных частей является не только отличительными признаками того или иного производителя устройства, но и тщательно продуманной стратегией безопасности.

В сфере мошенничества электронных платежей при обращении с кредитными картами, невозможно выделить единичную причину позволяющую совершать преступление. Так угрозы в виде «кардинга», «фишинга», пользования украденной (утерянной) картой, заявление от чужого имени и др. содержат в себе как социальные аспекты, так и уязвимости программного обеспечения и самого устройства терминала.

Эффективной мерой противодействия, в данном случае, является обучение клиентов банковских терминалов правилам пользования терминалов и мерам безопасности при обращении с картами электронных платежей, а так же своевременное их уведомление о выявленных опасностях.

Переходя с использования в своих банкоматах OS/2 на применение Windows и IP-сети, банки соответственно в корне меняют и систему подключения к своим информационным сетям. Во многих случаях это означает, что банкоматы и обычные офисные компьютеры банков оказываются подключенными к одним и тем же вычислительным сетям. Как следствие, сети банкоматов, инфокиосков, обменных пунктов и др. могут быть подвержены всем существующим видам угроз – вирусным атакам, злонамеренным действиям персонала, ошибкам администраторов, проникновениям изнутри и т.д.

Пути решения проблемы лежат в четком планировании и проектировании строящейся сети терминалов с учетом современных тенденций развития телекоммуникационных сетей, а так же использовании передовых технологий защиты информации: межсетевого экранирования; шифровании трафика; организации системы антивирусной безопасности и установки обновлений операционной системы; разработке политики безопасности функционирования системы; грамотном делегировании полномочий администраторов и обслуживающего персонала и др.

Следует так же учитывать тенденцию унификации электронных платежных сообщений и объединение в одну платежную систему ранее разрозненных организаций, что с упрощением взаимодействия между финансовыми учреждениями, в то же время, создает предпосылки для новых угроз безопасности.