ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОНЕЧНЫХ БАНКОВСКИХ ТЕРМИНАЛОВ

А.Н. ПАРХИМОВИЧ

Предложение банковских продуктов 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.

Данный процесс требует к себе особого внимания как со стороны правового обеспечения его функционирования, так и со стороны обеспечения безопасности при работе и эксплуатации терминалов.

Существующая в Республике Беларусь 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.

Правовую основу функционирования системы составляют Банковский кодекс Республики Беларусь, нормативные правовые акты Национального банка, а также разработанные в соответствии с ними локальные нормативные правовые акты и договоры банков и иных участников систем расчетов с использованием электронных платежных инструментов.

Системы расчетов с использованием электронных денег поддерживаются соответствующими техническими, организационными и процедурными мерами защиты для предотвращения, сдерживания и обнаружения угроз безопасности системы, в том числе и злоумышленных действий.

Программные и технические средства, применяемые в системах расчетов с использованием электронных денег, подлежат сертификации органом по сертификации программно-технических средств в области банковских услуг и технологий в порядке, установленном законодательством Республики Беларусь.

В целях обеспечения безопасной и надежной деятельности при осуществлении операций с электронными деньгами банки должны соблюдать нормативы безопасного функционирования и выполнять резервные требования, установленные Национальным банком.

Техническая, организационная и информационная поддержка развития функционирующих в Республике Беларусь систем расчетов с использованием банковских пластиковых карточек осуществляется ОАО "Национальный процессинговый центр", ЗАО "Платежная система "БелКарт".

Под безопасностью системы банковских терминалов понимают их свойство, выражающееся в способности противодействовать попыткам нанесения ущерба владельцам и пользователям системы при различных возмущающих (умышленных и неумышленных) воздействиях на нее. Иными словами под безопасностью системы понимается ее защищенность от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, модификации или разрушения ее компонентов. 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.

На сегодняшний день существует достаточно широкий спектр возможных злонамеренных действий, детектируемый на различных уровнях классификации угроз информационной безопасности и с каждым годом он расширяется.

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 видео наблюдения, 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.

Скимминг — вид мошенничества, при котором используют специальные виды электронных устройств, устанавливаемые на лицевой части терминала, для считывания информации о платежной карточке (номер карточки, пин-код), так считывающее устройство накладывается поверх гнезда для ввода карточки (закамуфлированные сканеры) и клавиатуры (накладные клавиатуры).

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.

Сети современных крупных банков уже нельзя назвать локальными в традиционном значении этого слова. Они состоят из множества подсетей и сегментов, распределенных территориально и объединяемых самыми различными каналами связи – от оптических до коммутируемых. 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 (в 2003 г. вирус Slammer заставил прекратить работу сразу 13 000 банкоматов Bank of America, Imperial Bank of Commerce), 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;

– шифрации 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.