# ПО банкомата: защита целостности

**Владимир Гуськов**
Руководитель отдела технической поддержки компании SafenSoft

Активная работа в России международных и национальных платежных систем, одобрение регуляторами развития электронных средств платежа привело к росту популярности карточных операций, расширению сетей банкоматов. Банкоматы в России представлены несколькими фирмами: Diebold, NCR и Wincor, иногда встречаются BenQ. Но каковы бы ни были их технические и программные характеристики, все они привлекают к себе внимание лиц, стремящихся к незаконному обогащению.

Современный банкомат вполне надежно защищен и от воздействия внешней силы, и от хакерских угроз, но разнообразные попытки взлома устройств для выдачи наличных не прекращаются. Статистика свидетельствует, что физические ограбления банкоматов значительно опережают «виртуальные» кражи по сумме наносимого ущерба, однако вряд ли это соответствует реальности — обнародование статистики «виртуальных» краж отрицательно влияет на репутацию банка. Конечно, не стоит забывать о таких методах как скимминг или траппинг, но они рассчитаны в первую очередь на невнимательность клиентов банкомата.

Нас же в первую очередь интересует защищенность персональной информации клиентов от хакерских угроз. Каковы же возможности компрометации клиентской информации злоумышленниками?

В первую очередь стоит назвать каналы связи, поддерживаемой между банком и банкоматом. Но все данные от банкоматов к банкам передаются в зашифрованном виде (сейчас для этого применяется 1024-битное шифрование). Не имея ключей шифрования, попасть в систему невозможно. Самой распространенной системой шифрования подобного рода является DESATM. Все данные шифруются непосредственно на банкомате, и весь путь следования проходят зашифрованными. Ключи, с помощью которых происходит шифрование, известны только банкомату и банковскому серверу, между которыми идет обмен. Впрочем, возможен вариант, когда подобные системы не используются, и в открытом виде не передается лишь PIN-код, а вся сопутствующая информация (номер карточки, данные держателя карты и т. д.) остается незашифрованной. В таких случаях ошибка банка заключается в том, что на банкоматах не использовалось дополнительное криптографическое ПО.

Следующая возможность — нарушение целостности ПО на банкомате.

Одним из важнейших факторов хищения информации с банкомата или платежного терминала является пользователь с правами администратора, т. е. ответственный за этот банкомат инженер. Такой пользователь может получить доступ непосредственно к информации обо всех клиентах, которые обращались к устройству самообслуживания: время и номер транзакций, проходящих через устройство, номер банковской карты, данные держателя карты и прочую критичную информацию. Пользователь, который имеет права администратора, может заразить операционную систему банкомата вирусами и троянами, что может привести к выводу устройства из строя или к хищению информации.

Отсюда следует, что для защиты целостности ПО и информации на устройствах самообслуживания необходимо специальное ПО, позволяющее защитить и осуществить контроль запуска и активности приложений, т. е. сохранить систему в исправном состоянии и не позволять ее модификацию. Необходимо защитить систему от случайного или умышленного инфицирования программами-шпионами через незащищенный доступ в сеть или при подключении нелегитимных носителей, например, USB-устройств, закрыть доступ к конфиденциальным данным у сотрудников с правами администратора. Желательно создание пользовательских правил активности приложений на устройстве самообслуживания, т. е. обеспечение контроля доступа различных приложений к файловой системе, ключам реестра, внешним устройствам и сетевым ресурсам.

Тогда ПО, необходимое для использования банкомата по прямому назначению, сможет проявлять ту и только ту активность, которая для этого необходима, все остальные операции, не санкционированные системой защиты, будут пресекаться, а злоумышленнику не останется никакой лазейки для воздействия на систему в своих интересах.