УСТРОЙСТВО ЗАЩИТЫ БАНКОМАТОВ С ВНЕШНИМ ИЗЛУЧАТЕЛЕМ ЭЛЕКТРОМАГНИТНОГО ПОЛЯ

Институт информационных технологий БГУИР, г.Минск, Республика Беларусь

Райко В. В.

Охрименко А. А. – канд. техн. наук, доцент.

Одним из самых опасных видов мошенничества в последние годы остается скимминг, при котором мошенники устанавливают на банкоматы считывающие устройства «скиммеры». Однако технологии банков не стоят на месте и уже разработаны и активно используются эффективные способы борьбы со скиммингом,

Устройство защиты банкоматов предназначено для препятствования так называемых скимминговых атак, сутью которых является незаконное получение информации, содержащейся на платежной карте, с использованием технических средств для считывания магнитной дорожки платежной карты и одновременным получением информации о вводимом PIN-коде клиента.

Принцип действия устройства строится на создании электромагнитного защитного поля, исключающего возможность считывания и дальнейшей передачи информации с карты на приемник злоумышленника.

Данное антискимминговое устройство содержит следующие компоненты:

- внутренний блок, в который входят: микроконтроллер, блок создания поля для излучателя, блок обработки и анализа атак на банкомат;
- экран для вывода информации;
- внешние коммутационные разъемы (разъем питания устройства, разъем для подключения излучателя, разъем для подключения модуля обнаружения атак);
- внешний излучатель поля.
- модуль обнаружения атак с датчиками обнаружения посторонних предметов и открытия банкомата.

В микроконтроллер входят: блок энергонезависимой памяти и блок обработки и анализа атак, второй микроконтроллер служит для генерации импульса защитного поля. Блок энергонезависимой памяти реализован как флеш-устройство, не требующее постоянного подключения к источнику питания. Блок создания поля реализован как колебательный контур.

Модуль обнаружения атак на банкомат состоит из следующих датчиков:

- магнитоконтактный датчик открытия дверей банкомата;
- датчик установки накладки (скиммера), который реализован как емкостной датчик, который предварительно калибруется, а в случае установки накладки (скиммера) меняется его емкость);
- датчик блокировки шторки штатного кард-ридера (попытка блокировки определяется путем анализа времени открытия и закрытия шторки, (в случае отличия данного интервала от заранее заданного определяется нештатный режим ее работы);
- датчик вандального воздействия на банкомат, который реализован как вибродатчик.

Данное исполнение позволяет осуществлять автономный мониторинг и анализ журнала атак; при отключении внешних источников питания записи об атаках и других важных событиях, совершенных с банкоматом, не теряются;

В качестве материала для сердечника внешнего излучателя использован молибденовый пермаллой. После установки базового корпуса устройства в корпус банкомата и размещения внешнего излучателя поля в непосредственной близости от щели приема карт банкомата, устройство включается и начинает, посредством внешнего излучателя, непрерывно создавать защитное поле. Радиус действия излучаемого поля 15 см. После того, как пользователь банкомата помещает карту в штатный считыватель банкомата, банкоматом посредством сигнала со шторки кард-ридера, подается команда на отключение защитного поля устройства; устройство автоматически отключается и не включается до того момента, пока карта находится в банкомате; устройство включается сразу после удаления карты из банкомата.

Таким образом, при использовании злоумышленниками так называемой «накладки» на приемное устройство банкомата и считывание ими информации с карты в момент, пока она не попала в штатное устройство банкомата, невозможно, чему препятствует созданное устройством защитное поле.

В случае попыток несанкционированного доступа к банкомату, а именно: попыток открывания двери банкомата, установки накладки (скиммера), блокировки шторки штатного кард-ридера, вандального воздействия на банкомат, сигнал с соответствующего датчика открывания двери поступает на устройство и записывается в энергонезависимую память, а также по сети передается на центральный пульт охраны.

Список использованных источников:

1.Алексанов, А.К. Безопасность карточного бизнеса: бизнес энциклопедия. / И.А.Демчев, А.М.Доронин, - Москва, 2012. - 432с.

2.Цветнов, В.В. Радиоэлектронная борьба. Радиомаскировка и помехозащита. / В.П.Демин, В.И.Куприянов. - Москва, 2012. – 240 с.