

ЗАХИЩЕНІСТЬ БАНКОМАТУ ТА ПЛАТІЖНИХ КАРТОК ВІД ЗЧИТУВАННЯ ІНФОРМАЦІЇ З МАГНІТНОЇ СМУГИ

Вступ. В Україні банкомати використовують не так вже і давно, типи банкоматів: NCR серії 56XX, 58XX, 66XX (Англія, Шотландія); Wincor 2000XE, 2050XE, 2100XE (Германія); Diebold Ortela (США). За цей час було чимало спроб порушити систему захисту банкомату з ціллю здобуття інформації про рахунок та вилучення коштів.

Основна частина. Одними з способів порушення системи захисту інформації є зчитування магнітної полоси з банківської картки.

Для захисту від зчитування магнітної полоси використовують антискіммінгові накладки з метою зниження ризику несанкціонованого доступу до персональних даних та попередження клієнтів про можливість встановлення накладок на клавіатурі або картридері банкомата. Антискіммінг, в свою чергу, буває:

1. Пасивним. Одним з апаратних засобів захисту від несанкціонованих маніпуляцій з картридером, широко застосовуваним сьогодні як штатної опції більшістю виробників АТМ, є установка на картридер захисної накладки, що закриває робочу область перед картридером і перешкоджає встановленню будь-якого стороннього пристрою, включаючи скімінг-пристрої. Накладка з'єднана кабелем з датчиком диспенсера банкомата. У разі видалення накладки шахраєм для встановлення на картридер скімінг-пристрою спрацьовує датчик на розмикання ланцюга живлення і банкомат відправляє на процесинг сигнал про помилку диспенсера та автоматично виводиться в режим «out of service».

2. Активним. Використовують пристрій, який монтується з внутрішньої сторони панелі обслуговування терміналу і підключається до модуля спеціальної електроніки банкомата. Принцип дії цього пристрою ґрунтується на постійному скануванні електромагнітного поля в області захисної шторки картридера. Як відомо, будь-який сторонній пристрій генерує навколо себе електромагнітне поле. Зміна стану електромагнітного поля в області захисної шторки картридера фіксується датчиками, після чого спрацьовує внутрішня сигналізація антискіммінгового пристрою. У разі знаходження стороннього пристрою в полі дії датчиків більше трьох хвилин відбувається спрацьовування комплексу і в процесинговий центр відправляється повідомлення про фатальну помилку картридера, потім банкомат виводиться з режиму обслуговування. Тим самим унеможливується незаконне копіювання інформації з платіжних карток.

Додатково, наприклад, у банкоматах Wincor використовується зміна швидкості зчитування інформації з картки, що підвищує безпеку.

Висновок. Система антискіммінга дозволяє фіксувати спроби впровадження в банкомат різних механічних (скріпки, цвяхи тощо) та електронних шахрайських пристроїв (сканерів). Також, значно підвищити безпеку використання банкомата також допомагає встановлення сертифікованого програмного забезпечення.