XXXI Студенческая международная заочная научно-практическая конференция «Молодежный научный форум: общественные и экономические науки»

КОЛИЧЕСТВЕННАЯ ОЦЕНКА ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ АНТИСКИММИНГОВОГО УСТРОЙСТВА ЗАЩИТЫ ОТ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

Эсмурзиева Хава Исаевна

студент 3-го курса Ингушского государственного университета, направления «Финансы и кредит», РФ, Республика Ингушетия, г. Назрань

Цурова Лиза Ахмедовна

научный руководитель, доцент Ингушского государственного университета, РФ, Республика Ингушетия, г. Назрань

Становление высокоэффективной экономики невозможно без развитого финансового рынка, составной частью которого является рынок банковских услуг.

В условиях серьезной конкуренции расширение круга клиентов неразрывно связано с постоянным поиском новых форм их обслуживания. Широкое поле для деятельности предоставляет в этом отношении работа с банковскими картами. Такой эффективный инструмент для кредитных организаций, с учётом последних российских и общемировых тенденций, всё более становится уязвимым для мошенничества с использованием пластиковых карт и сферы компьютерной информации.

Банковская карта - вид платежной карты, эмитированной кредитной организацией-эмитентом и предназначенной для совершения ее держателем операций, расчеты по которым осуществляются в соответствии с договором, заключенным с кредитной организацией-эмитентом.

Механизм функционирования системы безналичных расчетов основан на применении банковских карт и включает в себя операции, осуществляемые при помощи банкоматов, электронные системы расчетов населения в торговых организациях, системы банковского обслуживания клиентов на дому и на рабочем месте. В сфере денежного обращения банковские карты являются одним из прогрессивных средств организации безналичных расчетов.

Создание заинтересованности у физических и юридических лиц в переходе на безналичные расчеты при совершении повседневных платежей - отличная возможность для банков расширить круг своих клиентов, получить «дешевые» привлеченные средства и дополнительные источники доходов от их использования, а также свой процент (комиссию) от обслуживания безналичных платежей.

Сегодня любой банк во всем мире выполняет три основные функции: сбор денежных средств, их перемещение, и кредитование ими. Сбор денежных средств сам по себе стоит банку денег, на перемещении средств уже можно зарабатывать, основным же бизнесом банка является предоставление кредитов.

С помощью банковской карты вполне возможно построить банковские продукты, которые позволят успешно реализовывать банковский бизнес, соединяя воедино все три функции: собирая дешевые ресурсы большого числа «небогатых» клиентов, контролируя передвижение денег по циклу банковский счет - клиент - магазин - банковский счет, и кредитуя как физических, так и юридических лиц.

При выдаче карты клиенту осуществляется ее ***персонализация*** - на нее заносятся данные,

позволяющие идентифицировать карту и ее держателя, а также осуществить проверку платежеспособности карты при приеме ее к оплате или выдаче наличных денег. Процесс утверждения продажи или выдачи наличных по карте называется ***авторизацией***. Для её проведения точка обслуживания делает запрос платежной системе о подтверждении полномочий предъявителя карты и его финансовых возможностях.

Банкомат (от *банковский автомат*, иногда **ATM** от англ. *Automated teller machine*) — программно-технический комплекс, предназначенный для автоматизированных выдачи и приёма наличных денежных средств как с использованием платёжных карт, так и без, а также выполнения других операций, в том числе оплаты товаров и услуг, составления документов, подтверждающих соответствующие операции. Растет популярность банкоматов, оборудованных модулем по *приёму* наличных денежных средств, который позволяет пополнить карточный счёт, погасить задолженность по кредиту без посещения отделения банка. Банкомат снабжен устройством для чтения карты, а для интерактивного взаимодействия с держателем карты - также дисплеем и клавиатурой. Также, банкомат оснащен персональной ЭВМ, которая обеспечивает управление банкоматом и контроль его состояния. Последнее весьма важно, поскольку банкомат является хранилищем наличных денег. Современное большинство моделей рассчитано на работу в on-line режиме с картами с магнитной полосой, однако появились и устройства, способные работать со смарт-картами и в off-line режиме. Для обеспечения коммуникационных функций банкоматы могут оснащаться сетевыми платами или модемами.

Денежные купюры в банкомате размещаются в кассетах, которые, в свою очередь, находятся в специальном сейфе. Число кассет определяет количество номиналов купюр, выдаваемых банкоматом. Размеры кассет регулируются, что дает возможность заряжать банкомат практически любыми купюрами.

Основным направлением действий мошенников в отношении использования банкоматов является *скимминг*.

Скимминг – это действия мошенников в отношении использования скиммингового оборудования, представляющего собой устройства считывания информации с пластиковых карт и действующего в on-line и off-line режимах. В качестве примера такого оборудования продемонстрированы образцы, изъятые у мошенников Управлением Безопасности ОАО «Сбербанк России».

В большинстве случаев скимминговые устройства изготавливают в виде конструктивных элементов банкоматов, предавая им характерный внешний вид с помощью соответствующего лакокрасочного покрытия, нанесения логотипов и рекламных изображений.

Задача скимминговых устройств:

· перехват пин-кода карты;

· захват информации о данных банковской карты;

· получение перехваченных данных.

Перехват пин-кода карты осуществляется с помощью изготовления фальш-клавиатуры, конструкция которой выполнена таким образом, что при нажатии на её кнопки прилагаемые усилия передаются на кнопки настоящей клавиатуры. Однако в момент нажатия на кнопки происходит регистрация номеров кнопок и последовательность их нажатия

Перехват информации о данных банковской карты происходит с помощью специализированного оборудования, изготовленного в виде картоприёмника банкомата, устанавливаемого перед настоящим картоприёмником в качестве накладки. В большинстве случаев интерпретация полученной информации происходит посредством специализированных микросхем, представляющих собой аналого-цифровой преобразователь. В результате преобразования получается информация в цифровом формате в виде последовательности логических уровней, соответствующая записанным на магнитной полосе данным. В этом формате информация пригодна для различных преобразований для передачи другим цифровым устройствам для её хранения или трансляции.

Антискимминговая защита – деятельность банка, направленная против устранения причин мошеннической деятельности с пластиковыми картами, связанной с хищением банковской информации.

Предлагается осуществлять мероприятия по усилению антискимминговой защиты комплексным образом. Во-первых, это установка дополнительного оборудования на банкоматы, во-вторых, создание постоянного высокотехнологичного видеонаблюдения, в-третьих, это проведение регулярного контроля сотрудниками безопасности функционирования данного оборудования и проверки банкоматов на наличие несанкционированных устройств. Заключительным этапом по обеспечению защиты банковской информации при пользовании банкоматом должно стать правило личной безопасности каждого пользователя, которое заключается в том, что при пользовании банкоматом необходимо создать личное пространство в радиусе от 1,5 до 2-х метров.

В качестве обширной рекомендации выступают два варианта усиления антискимминговой защиты с помощью установки дополнительного оборудования.

Первый вариант предполагает установку активного комплекта, представляющего собой устройство активного противодействия несанкционированному считыванию данных магнитной полосы пластиковых карт при их пользовании в банкоматах и прочих терминалах финансового самообслуживания. Принцип работы изделия заключается в создании направленных электромагнитных импульсных помех в районе картридера терминала, препятствующих доступу к карте всех несанкционированных устройств. Отличительной особенностью изделия является то, что «защитное поле» генерируется постоянно, при котором совершенно неважно, когда, куда и каким образом злоумышленник установит скиммер — своей цели он уже никогда не добьется!

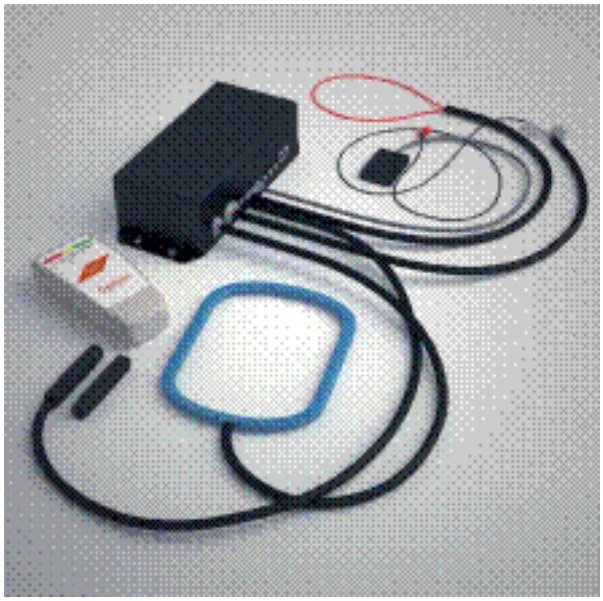

Рисунок 2. Активный антискимминговый комплект

Второй вариант защиты предполагает установить пассивный комплект – это пассивные Антискимминги Нового Поколения:

- Полностью прозрачные.
- Имеют новую уникальную форму.
- Щелевое отверстие для ввода карты заужено.
- Ударопрочные.
- Возможно нанесение логотипа банка.

Рисунок 3. Пассивный антискимминговый комплект

Все вышеперечисленные пункты, значительно усложняют и предотвращают, незаметную

установку и присоединение скимминговых устройств.

В действующем законодательстве не в полной мере учтены особенности современных видов мошенничества, что не позволяет обеспечить должную защиту интересов потерпевших. В конце 2012 года вступил в силу Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации». Анализ данного закона позволил сделать вывод о том, что суммы минимальных штрафов за мошенничество с платёжными картами (ст. 159^3), за мошенничество в сфере компьютерной информации (ст. 159^6) могут совсем не пугать мошенников в сфере компьютерной информации, что даёт возможность после вынесения судебного решения безбоязненно продолжать преступную деятельность. Стоит отметить, что данная статья содержит и другие меры наказания в виде лишения свободы, а также обязательных или исправительных работ. Но существует вероятность того, что правонарушитель при содействии настоятельного адвоката может просто «откупиться» без особо тяжких, в сравнении для дохода от его деятельности, затрат.

Таблица 1.

Ущерб от действия мошенников по данным Сбербанка России

2011год	2012год	2013год
341млн.	400млн.	432млн.

Таблица 2.

Сравнение затрат на покупку антискимминговогo оборудование с ущербом от мошенничества

Количество банкоматов	88 000 шт.
Установка активного комплекта	4000 шт.
Установка пассивного комплекта	84 000 шт.
Стоимость активного комплекта	37000 тыс.руб.
Стоимость пассивного комплекта	700 руб.
Всего затраты на активные комплекты	148 000 000 руб.
Всего затраты на пассивные комплекты	58 800 000 руб.
Итого затраты на покупку устройств	206 800 000
Сумма ущерба от мошенников за 2013г.	432 000 000 руб

По данным таблицы можно сделать вывод целесообразности антискимминговогo оборудования, т.к во всех доказанных случаях действий мошенников-скиммеров Сбербанк возвращает похищенные средства клиентам.

Сумма ущерба 432 000 000 руб > 206 800 000 руб. затрат на покупку устройств. Это еще раз доказывает высокую заинтересованность банков в приобретении антискимминговогo оборудования.

Антискимминговое оборудование легко устанавливается и обслуживается, а также является надежным, менее 1% сбоев на 3000 устройств по результатам 38 месяцев работы. Срок службы комплектов 5 лет.

Высокий темп роста объема платежей, совершенных через платежных и банковских платежных агентов, обусловлен в основном расширением перечня платежей, совершаемых через платежных и банковских платежных агентов. Около 70% от всех преступлений мошенников-скиммеров регистрируются в Москве и Московской области, что показывает целесообразность использование в этих регионах активного комплекта.

На примере города Москвы и МО таблица сравнение затрат на покупку антискиммингового оборудование с ущербом от мошенничества выглядит так:

Таблица 3.

Количество банкоматов	16 028 шт.
Установка активного комплекта	3000шт.
Установка пассивного комплекта	13 028шт.
Стоимость активного комплекта	37 000руб.
Стоимость пассивного комплекта	700 руб.
Всего затраты на активные комплекты	111 000 000руб.
Всего затраты на пассивные комплекты	9 119 600руб.
Итого затраты на покупку устройств	120 119 600руб.
Сумма ущерба от мошенников за 2013г.	302 400 000 руб

Расчет эффективности использования активного антискиммингового устройства:

· Цена активного комплекта 37000 тыс. рублей с НДС.

· Срок службы 5 лет.

Сумму ущерба - итоговые затраты на покупку устройств:

302 400 000 – 120 119 600 = 182 280 400

Из которых экономия 120 000 000 приходится на активные устройства по данным Сбербанка.

Таким образом делаем расчет эффективности:

Расчет строится на основе формулы $Iпрс = 1 + \frac{Э}{Ц}$;

$I = \frac{120000000}{3000}$ = 40 000 рублей в год, экономия на один банкомат

Срок службы * экономию на один банкомат в год

$$40\ 000 * 5 = 200\ 000$$

$$I\ прс = 1 + \frac{200000}{37000} = 6,4$$

Расчет эффективности использования пассивного антискиммингового устройства:

· Цена пассивного комплекта 700 рублей с НДС.

· Срок службы 5 лет.

Сумму ущерба - итоговые затраты на покупку устройств:

302 400 000 – 120 119 600 = 182 280 400

Из которых экономия 62 280 400 приходится на пассивные комплекты по данным Сбербанка.

Из вышеуказанных данных делаем расчет эффективности:

Расчет строится на основе формулы $1+\frac{Э}{Ц}$;

$I = \frac{62000000}{13028} = 4758$ рублей в год, экономия на один банкомат

Срок службы * экономию на один банкомат в год

$$4745 * 5 = 23790$$

$$I\,прс = 1 + \frac{23790}{700} = 34,9$$

$$Упрс = \frac{6,4*3000*37000+34,9*13028*700}{3000*37000+13028*700} = \frac{710400000+318274040}{111000000+9119600} = \frac{1028674040}{120119600} = 8,56$$

Таким образом использовав новую систему оценки эффективности можно сказать что Сберрбанк на каждый затраченный 1 рубль экономит 7 рублей.

Список литературы:

1. «Антискимминг в действии» - http: //www.chclub.ru.

2. АТМ-фрод: кто виноват и что делать? Скимминг, пассивный антискимминг и антискимминговые. Журнал ПЛАС № 2 (122) 2007- http: //www.plusworld.ru/journal/online/art140118/.

3. Барышева А. Инновационный менеджмент. – М.: Дашков и Ко, 2012.

4. Дмитрий Саливон. Миллионы на защиту: новое в технологиях антискимминга (опыт России). http: //www.prostobankir.com.

5. Москвин, В.А. Управление качеством в бизнесе: рекомендации для руководителей предприятий, банков, риск- менеджеров / В.А. Москвин. - М.: Финансы и статистика, 2006. - 384 с.