УДК 336.71.078.3

Богданова Юлия Вячеславовна

бакалавр направления «Экономика»
Российская академия народного хозяйства и государственной службы при Президенте РФ
Челябинский филиал
Россия, Челябинск

bogdanovaulia1234@gmail.ru

Julia V. Bogdanova

Bachelor of Economics
Russian academy of national economy and public service under the President of the Russian Federation
Chelyabinsk branch
Russia, Chelyabinsk

Сомова Наталья Леонидовна

бакалавр направления «Экономика»
Российская академия народного хозяйства и государственной службы при Президенте РФ
Челябинский филиал
Россия, Челябинск

natasha.somova.99@mail.ru

Natalya L. Somova

Bachelor of Economics
Russian academy of national economy and public service under the President of the Russian Federation
Chelyabinsk branch
Russia, Chelyabinsk

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ [1]

BANK CARD FRAUD

Аннотация

В статье рассматривается суть мошенничества с банковскими картами, различные его виды. Проводится анализ количества краж с банковских карт клиентов, объем причиненного ущерба. Рассказывается о возможных мерах наказания для мошенников в случае незаконного изъятия денежных средств у владельцев банковских карт, а также о способах защиты своих банковских карт от мошеннических действий.

Ключевые слова:

банковские карты, мошенничество, скимминг, фишинг, SMS-мошенничество, поддельные банкоматы

Abstract

This article discusses in detail the essence of bank card fraud, its various types. The analysis of the number of thefts from bank cards of customers, the amount of damage caused. It describes possible penalties for fraudsters in the event of illegal withdrawal of funds from bank card holders, as well as ways to protect their bank cards from fraudulent activities.

Keywords:

cards, fraud, skimming, phishing, SMS fraud, fake ATMs

Введение: Проблема мошенничества с банковскими картами является актуальной. В настоящее время в мире в обращении находится около миллиарда банковских пластиковых карт. Их внедрение является важнейшей тенденцией развития технологии безналичных расчетов в банковской деятельности, что в свою очередь и привлекает внимание мошенников, охотившихся за чужими денежными средствами путем обмана и злоупотребления доверием. Это связано с тем, что

[1] Научный руководитель: Коротина Наталья Юрьевна, доцент, кандидат экономических наук, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Челябинский филиал

большинство молодых и взрослых людей, имеющих банковские пластиковые карты, мало знакомы с видами мошенничества и способами защиты от него.

Цель: Главная задача данной статьи заключается в подробном изучении структуры мошенничества с банковскими картами, а также анализе объема ущерба и изучении ловушек мошенников. Ну и самое главное в способах защиты банковских карт от мошенников, охотившихся за чужими деньгами.

Методы исследования: Методологической основой исследования послужили как теоретические (методы структурного и функционального анализа, синтез) так и практические методы познания (сравнение, прикладной анализ, описание).

Мошенничество — хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием. Лицо, занимающееся этим, называется мошенник или мошенница [1].

Карты как финансовый инструмент постоянно совершенствуются, растет сфера их применения, расширяется комплекс оказываемых услуг с их использованием.

Как и всякий высокодоходный бизнес, а в особенности в сфере денежного оборота, банковские пластиковые карты давно стали мишенью для преступных посягательств.

Существует достаточно много способов мошенничества с банковскими картами. Основными из них являются [2]:

1) Мошенничество с банкоматами (скимминг, банкоматы-фантомы, шимминг, скотч-метод);

2) Мошенничество при расчетах за покупки в супермаркете, торговом комплексе с помощью банковских карт;

3) Мошенничество при оплате безналичных счетов в гостиницах, кафе;

4) Воровство данных кредитных картах с помощью вирусов на компьютере;

5) Мошенничество с банковскими картами во время покупок товаров через интернет;

6) Обман владельца банковской карты по телефону/SMS.

По данным исследования компании «Информзащита» [3], число интернет–краж с карт в 2018 году достигло 315 тыс., а объем ущерба – 1,3 млрд рублей. Годом ранее мошенники скомпрометировали 300 тыс. краж, ущерб составил 1,05 млрд рублей. В 2016 году – 267 тыс. краж, ущерб – 1,08 млрд руб., в 2015 году – 257,7 тыс. краж, ущерб – 1,78 млрд руб. (табл. 1).

Таблица 1 – Число интернет краж с банковских карт

Год	Число интернет-краж, тыс. шт.	Темпы роста интернет - краж, %	Объем ущерба, млрд руб.	Темпы прироста объема ущерба от интернет - краж, %
2015	257,7	329,5	1,78	12,66
2016	267	3,61	1,08	- 39,3
2017	300	12,36	1,05	- 2,78
2018	315	5	1,3	23,81

По мошенничеству с пластиковыми картами реальная статистика отсутствует, т.к., во-первых, банки не стремятся выносить на всеобщее обозрение свои потери от мошенников, не хотят портить репутацию, а во-вторых, сами люди, пострадавшие от преступных действий, не спешат обращаться в полицию: или суммы потери невелики, или надежды на результат нет. Таким образом, статистика по данному вопросу бывает официальной, т.е. по данным МВД, и неофициальной, т.е. по обрывкам информации, которая появляется в интервью с разными должностными лицами.

К основным видам мошенничества с банковскими картами относятся: скимминг, фишинг, SMS-мошенничество, кража денег с бесконтактных карт, поддельные банкоматы.

Скимминг – это копирование данных банковской карты с помощью специальных устройств – скиммеров. Такие устройства устанавливаются в картоприемники банкоматов.

Для защиты от скиммеров на банкоматы часто устанавливают защитные вставки – антискиммеры. Они выглядят как круглые устройства из полупрозрачного зеленого пластика, которые вставляются в картоприемники.

Фишинг – это вид мошенничества, который заключается в том, чтобы достать реквизиты карты обманным путем. Чаще всего его используют в интернете, но иногда он применяется и в реальной жизни.

Похоже на фишинг выманивание данных карты по телефону под каким-либо предлогом. Мошенник может представиться сотрудником банка, который потребует сообщить реквизиты карточки и PIN-код – например, чтобы разблокировать ее.

SMS-мошенничество – это способ, при котором вы получите на свой телефон сообщение с подозрительным содержанием. Цель у него, как и у фишингового сайта – заставить человека тем или иным способом сообщить мошеннику реквизиты карты.

Например, вам приходит сообщение о том, что вы выиграли в каком-либо розыгрыше призов. Но, чтобы забрать награду, вам нужно отправить некоторую сумму на счет организатора – например, заплатить за доставку.

Кража денег с бесконтактных карт – это действия представляют угрозу для карт, которые поддерживают бесконтактную технологию оплаты – PayWave от Visa и PayPass от MasterCard. Такие карточки не обязательно вставлять при оплате в платежный терминал. Достаточно поднести их к устройству на несколько секунд.

Поддельные банкоматы – это способ мошенничества, встречающийся редко из-за того, что поддельный банкомат стоит очень дорого. Однако, на него все еще можно попасться. Поддельные банкоматы ставятся в местах, где нет какой-либо охраны или камер. Такое устройство внешне очень похоже на оригинальное, но сильно отличается внутренней «начинкой» [4].

Основными проблемами в безопасности пластиковых карт выделяем следующие:

1) Оплата, не требуемая вставлять карту в чип-ридер.

Конечно, современные карты оснащены специальным чипом, который практически невозможно скопировать. Однако магнитная полоса на них по-прежнему есть. Терминалы оплаты в некоторых торговых точках позволяют произвести оплату только с помощью магнитной полосы, не требуя вставлять карту в чип-ридер для считывания информации с чипа.

2) Необязательный ввод ПИН-кода для совершения покупок.

Нужно ли обязательно вводить ПИН-код для совершения покупки или достаточно просто расписаться на чеке – определяет не плательщик, а владелец платёжного терминала.

3) Незащищенные интернет-платежи.

Банки, выпускающие карты, которые поддерживают технологию 3D-Secure (Verified by Visa и MasterCard SecureCode), особо подчёркивают, что их карты позволяют совершать покупки онлайн более безопасно. Это, конечно, так, 3D-Secure предполагает дополнительную ступень защиты: для совершения покупки требуется ввести пароль, который приходит Вам по смс. Однако недостаточно, чтобы Ваша карта поддерживала функцию 3D-Secure, нужно чтобы и интернет-магазин также её поддерживал. Есть множество сайтов, где 3D-Secure просто не используется (Aliexpress, например) [5].

В Российской Федерации действуют следующие меры наказания за мошенничество с пластиковыми картами.

Наказания для тех, кто проводит мошеннические действия с банковскими картами, определяет статья 159.3 Уголовного кодекса РФ. Она устанавливает разную ответственность для преступников в зависимости от тяжести причиненного вреда [6].

Таблица 2 – Меры наказания за мошенничество с банковскими картами

Характеристика преступника и размер ущерба	Мера наказания
Одно лицо	Штраф до 120000 рублей Обязательные работы на срок до 360 часов Исправительные работы на срок до года Ограничение свободы на срок до двух лет Принудительные работы на срок до двух лет Арест на срок до четырех месяцев
Группа лиц по предварительному сговору	Штраф до 300000 рублей Обязательные работы на срок до 480 часов Исправительные работы на срок до двух лет Принудительные работы на срок до пяти лет с ограничением свободы на срок до года или без него Лишение свободы на срок до пяти лет
Лицо, наделенное служебными полномочиями и ущерб в особо крупном размере	Штраф до 500000 рублей Принудительные работы на срок до пяти лет с ограничением свободы на срок до года или без него Лишение свободы на срок до пяти лет со штрафом до 80000 рублей или без него
Организованная группа лиц или ущерб в особо крупном размере	Лишение свободы на срок до десяти лет со штрафом до 1000000 рублей или без него

В Российской Федерации также имеются способы защиты банковских карт от мошенников.

Существует ряд общепринятых правил, которые следует применять во время пользования пластиком, чтобы обеспечить безопасность банковских карт:

Физические способы защиты данных карты: Как уже было описано выше, на карте нанесено достаточно данных для кражи с неё денег. Сфотографировать обе стороны карты на смартфон можно за пару секунд, ненамного дольше копируются данные магнитной полосы с помощью специального оборудования. Поэтому нельзя оставлять свою карточку без присмотра.

Не разглашать третьим лицам данные карты: никогда не сообщайте данные карты по телефону, электронной почте и т.д. Очень часто мошенники под видом

сотрудников банка требуют уточнить какую-либо информацию или проделать определенные действия, чтобы отменить ошибочную операцию. Предлоги бывают самые разные: технический сбой, проверка системы, несанкционированный доступ, обнаружение ошибки при заполнении анкеты и т.д.

Электронные способы защиты: К ним, прежде всего, относится базовая защита оборудования [7]:

1) установка лицензионного антивируса на домашний компьютер и смартфон;

2) нельзя переходить по подозрительным ссылкам, открывать электронные письма от неизвестных лиц;

3) не используйте незащищенные wifi-сети;

4) регулярно обновляйте пароль доступа к интернет-банку, составляя комбинацию из строчных и заглавных букв, цифр и символов и др.

Деятельность Банков по защите банковских карт клиентов от мошенничества заключается в том, что банки разрабатывают системы и способы защиты банковских карт от мошенников. Так, один из самых популярных банков в РФ– Сбербанк для защиты клиентской информации и противодействия мошенничеству при совершении операций на устройствах самообслуживания разработал новый стандарт. Стандарт включает защиту от скимминга (считывание информации с магнитной полосы с помощью специальных устройств), black box атак (подключение стороннего устройства к устройству выдачи денег) и Transaction Reversal Fraud (мошенничество при снятии наличных средств в банкомате с манипулированием карточного счета).

Помимо предложенного Сбербанком сервиса защиты карточек от киберугроз и установки антивирусной программы продукт содержит опции, покрывающие стандартные риски [8]:

1. Утеря карточки в результате обыкновенного механического повреждения, размагничивания, кражи, технической неисправности терминала или банкомата.

2. Хищение посторонними лицами денег, обналиченных через банкомат, в течение 2 часов после проведения операции.

3. Хищение денег различными способами при участии посторонних лиц (получение пластика и информации о ПИН-коде насильственным путем, копирование подписи картодержателя с платежных документов, использование поддельной карточки с реальными данными по действующей карте, снятие денег при помощи скимминга и фишинга).

Таким образом, рассмотрев сущность мошенничества с банковскими картами и исходя из проведенного анализа объема ущерба с 2015-2018 гг., в банках России требуется усовершенствование технологий по защите пластиковых карт, а также необходимо более глубокое изучения способов защиты карт от мошенников большинству молодых людей, которым впервые выдали пластиковую карту, а также и взрослым людям, которые имеют небольшой кругозор знаний о защите банковских карт и о возможности действий мошенников.

Список использованных источников

1. Википедия [Электронный ресурс] URL: https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE (дата обращения: 4.09.2019)
2. Виды мошенничества с банковскими картами – как могут украсть деньги с карты? [Электронный ресурс] URL: https://www.papabankir.ru/kreditnyye-karty/moshennichestvo-s-bankovskimi-kartami/ (дата обращения: 4.09.2019)
3. Алексеевских, А. ИЗВЕСТИЯ IZ [Электронный ресурс] URL: https://iz.ru/713533/anastasiia-alekseevskikh/vorovat-dengi-s-kart-stali-chashche-no-berut-menshe (дата обращения: 5.09.2019)
4. Мошенничество с банковскими картами и
5. способы защиты от него [Электронный ресурс] URL: https://vsezaimyonline.ru/sovety/moshennichestvo-s-kartami.html(дата обращения: 6.09.2019)
6. Мошенничество с банковскими картами: способы защиты. RODINA информационный блог [Электронный ресурс] URL: https://hranidengi.my1.ru/news/moshennichestvo_s_bankovskimi_kartami_sposoby_zashhity/2017-03-23-82 (дата обращения: 6.09.2019)
7. Мошенничество с банковскими картами и способы защиты от него
8. [Электронный ресурс]
9. URL: https://vsezaimyonline.ru/sovety/moshennichestvo-s-kartami.html (дата обращения: (7.09.2019)
10. Мошенничество с банковскими картами способы защиты.

11. [Электронный ресурс] URL: http://hranidengi.ru/moshennichestvo-s-bankovskimi-kartami-sposoby-zashhity/ (дата обращения: 8.09.2019)

12. Защита банковских карт Сбербанк. [Электронный ресурс] URL: https://sbankami.ru/uslugi/zashhita-bankovskix-kart-sberbank.html (дата обращения: 9.09.2019)