***Масленникова Анастасия Юрьевна***
канд. экон. наук, доцент
***Мандровицкая Мария Евгеньевна***
студентка
***Плотникова Александра Викторовна***
студентка
Уральский институт управления (филиал)
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте РФ»
г. Екатеринбург, Свердловская область

# МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

***Аннотация****: в данной статье представлено описание наиболее распространённых способов мошенничества с банковскими картами, а также рекомендации по обеспечению их безопасности и сохранности. Данная проблема является актуальной, учитывая растущий интерес граждан к данной форме хранения денежных средств.*

***Ключевые слова****: банковский сектор, мошенничество, банковские операции, банковская защита.*

В Положении ЦБ РФ от 24 декабря 2004 г. «Об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт» дается следующее определение: «Банковская карта – это инструмент безналичных расчетов, предназначенный для совершения операций с деньгами, находящимися у эмитента». Она отличается удобством обращения, возможностью многократного применения. С ее помощью можно осуществлять безналичную оплату товаров или услуг, а также получать наличные денежные средства в отделениях банков и банкоматах [1].

Ускорение темпа жизни требует от человека высокой скорости принятия решений и мобильности. Поэтому в современном мире банковские карты стали неотъемлемой частью жизни человека. Учитывая, как часто в работе и в рамках бытовых вопросов нам приходится сталкиваться с расчетными операциями,

ускорение денежного обмена посредством расчета банковской картой значительно сокращает трансакционные издержки. Это очень удобный способ оплаты, перевода средств на дальние расстояния. Без сомнения, карта стала отличной альтернативой банкнотам и монетам. Не нужно носить с собой наличные средства, когда всё можно уместить в небольшую пластиковую карту.

Также созданы банковские карты с NFC технологией, которая позволяет вам производить оплату без непосредственного контакта карточки с платежным терминалом. Требуется только поднести карту к терминалу, не вводя ПИН-код, и будет произведена оплата.

Однако любая система несовершенна, и именно эти, на первый взгляд незначительные, несовершенства становятся оружием в руках мошенников, что приводит к негативным последствиям. Появилось множество способов, с помощью которых мошенники могут украсть ваши деньги. За год владельцы банковских карт потеряли приблизительно миллиард рублей из-за действий аферистов. Кражи денег с каждым годом становятся всё изощрённее.

ГУ Банка России по ЦФО опубликовали статистику, в которой можно отметить, что объем несанкционированных операций с использованием платежных карты через Интернет и устройства мобильной связи является более масштабным. Например, в 2016 году объем составил 178.7 млн руб., а в 2017 увеличился и составил 181.6 млн руб. Это говорит о стремительном развитии мошенничества спустя всего год. Объем операций через банкоматы и платежные терминалы, наоборот, уменьшается с каждым годом. Например, в 2015 году он составил 65 млн руб., в 2016 43.9 млн руб., а в 2017 уже 26.5 млн руб. [4].

Множество операций совершаются за пределами Российской Федерации, что, несомненно, осложняет поиск злоумышленников, тем более привлечение их к ответственности.

Какие же способы используют мошенники? Пожалуй, каждый владелец банковской карты сталкивался с подозрительными СМС-сообщениями или звонками с просьбой сообщить свои персональные данные или реквизиты карты. Это два самых частых способа мошенничества, взятые на вооружение пре-

ступниками, которые идут в ногу со временем и развитием технологий. В настоящее время держатели пластиковых карт все чаще сталкиваются с угрозами при их использовании.

Наиболее актуальными способами получения денежных средств незаконным путем являются: СМС – мошенничество, мошенничество через e-mail или телефонные звонки, мошенничество при заказе товаров и услуг через интернет-магазин, мошенничество при расчётах пластиковой картой в магазине, а также установка нелегальных считывающих устройств на банкоматах и телефонах [3].

Самые простые способы мошенничества производят через СМС и e-mail. В данном случае, злоумышленники рассылают сообщения о блокировании карты, приостановке обслуживания по карте, изменении ПИН-кода, окончании срока действия карты и т. д. Далее указываются рекомендации направить информацию о реквизитах пластиковой карты. Стоит отметить, что банки никогда не осуществляет отправку СМС и e-mail с целью получения реквизитов держателя карты.

Стремительно разевается интернет-торговля, что даёт хорошие возможности для манипуляции с денежными средствами. При заказе товаров через интернет-магазин можно наткнуться на уведомление с просьбой ввести ПИН-код, что является одной из уловок мошенников. Для оплаты онлайн-покупок рекомендуется использовать виртуальную банковскую карту на определенную сумму и определенное количество покупок.

Мошенничество при расчётах пластиковой картой в магазине также имеет место быть. При оплате покупки сотрудники торговой точки могут скопировать реквизиты Вашей пластиковой карты и в дальнейшем, сделать её копию. Проведение операций с картой должно постоянно контролироваться её владельцем.

Возможна установка на банкоматах и мобильных телефонах нелегальных считывающих устройств. Для получения конфиденциальной информации о карте мошенники могут установить считывающие устройства над ПИН-клавиатурой и на устройство для приёма карты в банкомате.

Мошенники могут использовать нелегальные мобильные устройства для считывания данных с карт, поддерживающих технологию бесконтактной оплаты. В данном случае рекомендуется подключить услугу СМС-информирования об операциях по бесконтактной карте. Это позволит оперативно получать информацию обо всех операциях, совершаемых по карте.

С NFC-системой тоже нужно быть предельно аккуратными. Злоумышленнику достаточно приблизить считыватель к карте на расстояние 5–20 сантиметров, чтобы списать деньги. Это происходит в людных местах с большим скоплением людей. Злоумышленники прислоняют бесконтактный считыватель к наиболее очевидным местам хранения карты: карманы одежды, сумки и т. д. В целях безопасности рекомендуется носить дебетовую карту в специальном чехле.

Многие банки оставляют на официальных сайтах список рекомендаций по использованию банковской карты. Так, например, ПАО Сбербанк предоставляет пользователям инструкцию «Как безопасно пользоваться банковской картой». «Банковская карта – ключ доступа к вашему счету. Относитесь к ней так же бережно, как к наличным» [2], – с этих слов начинается данная инструкция. Несмотря на их простоту, они содержат в себе важный смысл. Большинство людей относятся к банковской карте менее внимательно, нежели к наличным деньгам. Карта легкая, имеет небольшой размер и позволяет не отсчитывать нужную для оплаты сумму. Можно сказать, что все эти характеристики усыпляют бдительность пользователя.

Если случаи атаки мошенников на банковский счет все же были обнаружены, карту рекомендуют немедленно заблокировать в отделении банка [5].

Несмотря на большое количество таких защитных механизмов, как СМС-уведомления об операциях по карте, отражение потоков денежных средств через онлайн-банк или возможность блокировки карты в случае ее утери или кражи, лучшей защитой платежных карт является внимательность и осторожность их владельцев.

***Список литературы***

1. Банковское право / И.В. Кушнир, 2010 [Электронный ресурс]. – Режим доступа: http://be5.biz/pravo/b010/39.html (дата обращения: 02.07.2019).

2. ПАО Сбербанк [Электронный ресурс]. – Режим доступа: https://www.sberbank.ru/ru/person/dist_services/warning/bezopas_card (дата обращения: 03.07.2019).

3. Правила выпуска и обслуживания банковских карт Банка «Снежинский» АО [Электронный ресурс]. – Режим доступа: https://www.snbank.ru/files/phi/cards/card_ugroza.pdf (дата обращения: 02.07.2019).

4. ФГБУ «Редакция «Российской газеты» [Электронный ресурс]. – Режим доступа: https://rg.ru/2018/04/17/5-osnovnyh-afer-s-bankovskimi-kartami-kak-ne-stat-zhertvoj-moshennikov.html (дата обращения: 02.07.2019).

5. Банковское законодательство: учеб. / под ред. Е.Ф. Жукова. – М.: Вузовский учебник, 2012.