Copyright © 2019 by Academic Publishing House Researcher s.r.o.

Published in the Slovak Republic
Vestnik policii
Has been issued since 2014.
E-ISSN: 2414-0880
2019, 6(2): 67-75

DOI: 10.13187/vesp.2019.2.67
www.ejournal21.com

Bank Card Fraud Types and Security

Vadim A. Smirnov [a, *]

[a] State university of the sea and river fleet of the name of the Admiral S.O. Makarov, Russian Federation

Abstract

This article is devoted to security issues in the use of bank cards and ATMs, as the conduct of monetary transactions with the use of cards has become an integral part of the life of almost every person and due to the ignorance and insensitivity of people, frauds actively use it. The schedule of issued cards and the number of thefts with their use are given, as well as a list of the main types of thefts and new tricks of criminals, for carrying out unauthorized transactions. The methods used by banks to combat crime are described and what needs to be done to increase the financial literacy of the population. It has been concluded that for the safety of their funds, it is necessary to adhere to several simple rules and to remember that bank card details cannot be reported to anyone and under any conditions.

Keywords: credit card, frauds, funds, unauthorized transaction, security, ATM.

1. Введение

В настоящее время трудно найти человека, у которого бы не было банковской карты, будь то кредитная или дебетовая, физическая или виртуальная. Многие используют больше одной карты от разных банков. Даже сотовые операторы стали выпускать собственные банковские карты. И с каждым годом, их количество только увеличивается.

По данным ЦБ РФ на 1 января 2019 года, количество банковских карт составляет 272 608 тысяч. По сравнению с 1 января 2008 года (103 041) количество карт выросло на 169 567 тысяч (+164,56 %) (ЦБ РФ; Рисунок 1).

* Corresponding author
E-mail addresses: vadimkasmi@mail.ru (V.A. Smirnov)

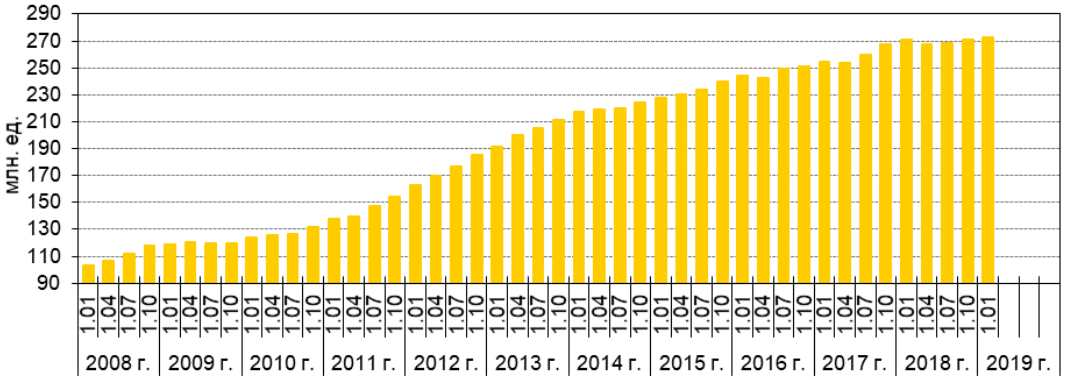

Рис. 1. Количество расчетных и кредитных карт, эмитированных кредитными организациями

По данным ВЦИОМ на 1 марта 2019 года, 87 % россиян стали чаще пользоваться банковскими картами за последние 4-5 лет (ВЦИОМ).

Вместе с тем и увеличивается объем несанкционированных операций с использованием платежных карт.

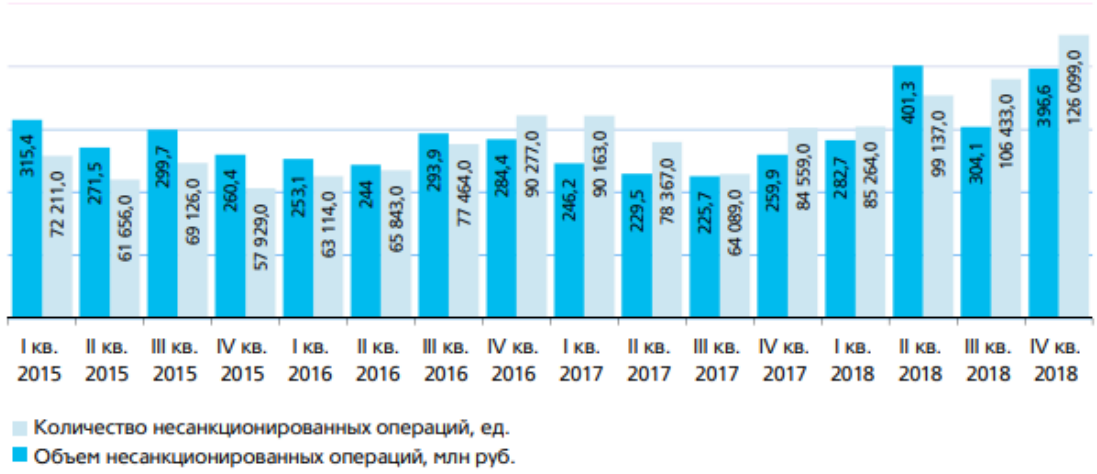

Рис. 2. Количество и объем несанкционированных операций с использованием платежных карт

По данным ФинЦЕРТ, объем всех несанкционированных операций, с использованием банковских карт выпущенных на территории РФ в 2018 году, составил 1384,7 млн рублей, что на 423,3 млн рублей (44 %), превышает аналогичный показатель за 2017 год – 961,3 млн рублей. Количество операций выросло с 317 178 тыс. единиц за 2017 год до 416 933 тыс. единиц за 2018 год (ФинЦЕРТ, 2018; Рисунок 2).

Мошенники проявляют огромную изобретательность, чтобы получить реквизиты банковских карт или прямой перевод денежных средств на свои счета. Для того чтобы обезопасить себя от кражи, следует знать наиболее распространение способы, которые используют злоумышленники.

2. Материалы и методы

В качестве материалов для исследования, использованы официально опубликованные данные Центрального Банка Российской Федерации, опросы Всероссийского центра изучения общественного мнения и Национального агентства финансовых исследований, отчеты Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере.

Основными методами, являются методы эмпирического исследования: наблюдение, сравнительный и логический анализ, эксперимент.

3. Обсуждение

Существует множество способов украсть денежные средства с карты, начиная с самого банального, кражи самой пластиковой карты и заканчивая перехватом данных с банкомата.

Казалась бы, как можно воспользоваться краденной картой, если неизвестен ПИН-код, а код для подтверждения интернет покупок приходит на мобильный телефон привязанный к карте. Самое простое, что может сделать мошенник, это просто подсмотреть ПИН-код, когда вы набираете его в банкомате или при оплате покупок в магазине. Так же, большое количество сайтов и приложений, не требует 3-D Secure для подтверждения оплаты.

Для примера возьмем два популярных сервиса: сайт для покупки товаров AliExpress и приложение для заказа такси Яндекс Такси. Зайдем на AliExpress и совершим покупку. Вводим: номер карты, Имя и Фамилию, Срок действия, CVV код (Рисунок 3). Нажимаем подтвердить и оформить заказ.

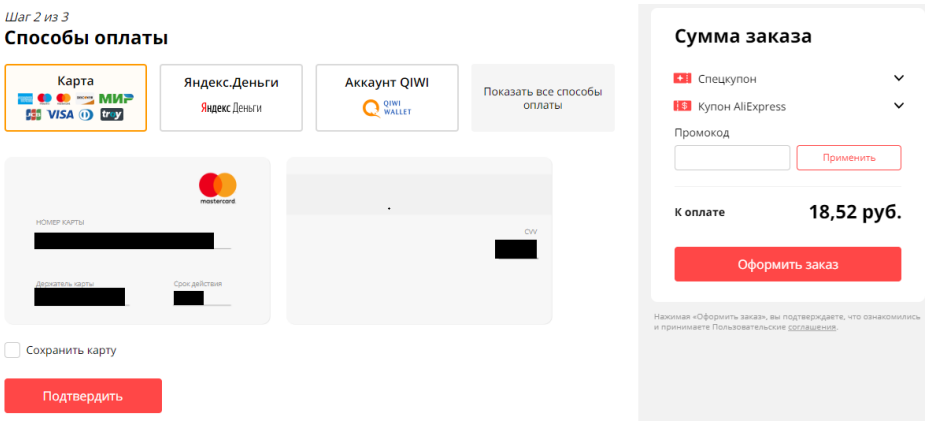

Рис. 3. Ввод данных карты

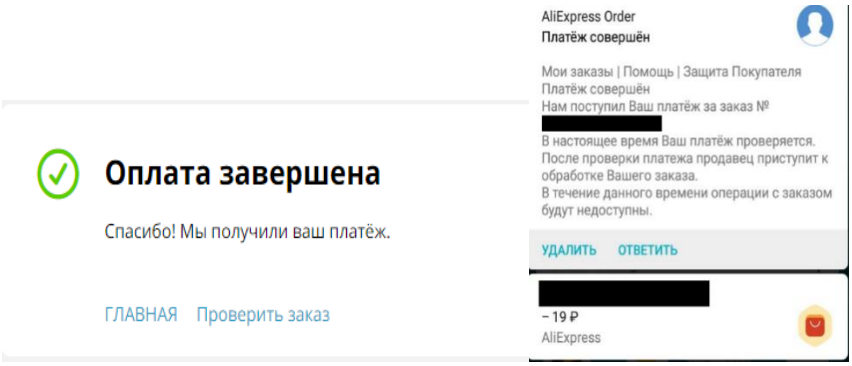

Рис. 4. Подтверждение платежа

Так же, зайдем в приложение Яндекс Такси, и добавим нашу карту. Проводим все те же манипуляции и все, карта привязана (Рисунок 5).

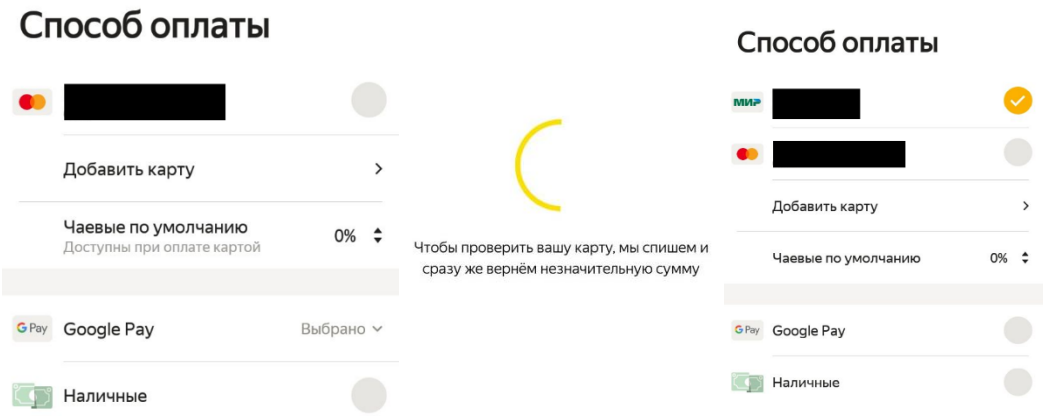

Рис. 5. Привязка карты Яндекс Такси

Все это происходит без использования 3-D Secure.

Еще один нехитрый способ, который может применить мошенник в случае, когда он владеет вашей картой – это использовать бесконтактную оплату. Трудно назвать банк, который не внедрил технологию бесконтактных платежей в свои карты. Плюсом и в то же время минусом этой технологии, является то, что при сумме покупок до 1 тыс. рублей подтверждать операцию ПИН-кодом не нужно. Однажды я сам столкнулся с этой проблемой. Когда заметил, что потерял карту, было проведено уже порядка трех платежей.

Дополнительным минусом бесконтактных платежей является невозможность оспаривания операций (Рисунок 6).

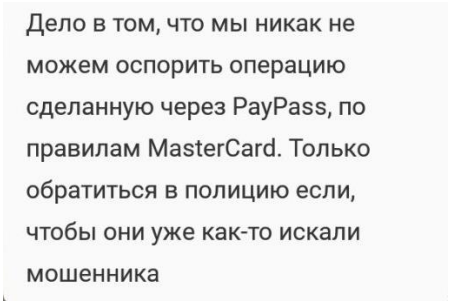

Рис. 6. Сообщение банка

В мае 2019 года стало известно еще об одном необычном способе кражи денежных средств с карт. Преступник, при помощи бесконтактной банковской карты выполнял перевод денег на номер телефона, но не завершал ее и отходил от банкомата. Следующий человек, подходивший к банкомату, вставлял банковскую карту, и система автоматически завершала предыдущую операцию, тем самым списывая со счета жертвы нужную сумму. После чего, через систему электронных платежей, украденные средства переводились на свой счет и в дальнейшем обналичивались (27.мвд.рф).

Когда ваша карта находится в руках преступника, ему не составит труда узнать ФИО. Да, на карте указывают только фамилию и имя, но что будет, если попробовать перевести некоторую сумму на ваш счет.

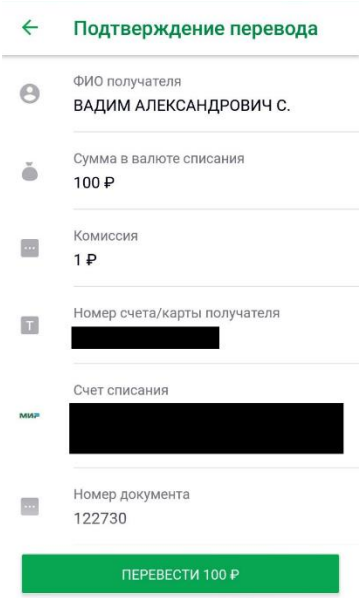

Рис. 7. ФИО жертвы

Сразу станет известно и ваше отчество (Рисунок 7). И тут мы переходим к наиболее популярному на данный момент способу кражи денежных средств, которым пользуются злоумышленники – социальная инженерия. На форуме «Финополис» первый заместитель директора Департамента информационной безопасности Банка России сказал: «Более 97 % хищений со счетов физических лиц и 39 % хищений со счетов юридических лиц были совершены с использованием приемов социальной инженерии».

Можно выделить 3 фактора успешной атаки:

1. Пробудить чувство страха из-за потери денег;
2. Использовать меркантильные качества человека;
3. Срочное сообщение информации (пример: в данный момент списывают деньги).

Выбрав одну из трех тактик или комбинируя их, можно побудить жертву к передаче банковских данных для дальнейшей кражи средств.

На самом деле, чтобы использовать этот метод, все что нужно знать это номер телефона клиента и ФИО. Эти данные можно купить на сторонних сайтах, благодаря многократным утечкам персональных данных. Только за последние два месяца стало известно о крупных утечках таких компаний как: Сбербанк, Альфа-Банк, ВТБ, Билайн. А также существует множество операторов обработки персональных данных, откуда так же происходят утечки.

На данный момент, злоумышленники стали чаще подменять свой мобильный номер, на номер банка, обзванивать клиентов и представляться сотрудниками службы безопасности банка. Сообщают, что сейчас происходит подозрительная операция по вашему банковскому счету, кто-то пытается вывести некоторую сумму денег, находясь в другом регионе и необходимо проверить вы это или нет. Услышав ответ “нет”, они просят вас в срочном порядке назвать те данные которые им нужны, в противном случае ваши деньги пропадут моментально. Ну и конечно, неосведомленный человек, опасаясь за свои сбережения, бездумно называет все, что его попросят. Или же говорят о том, что ваш родственник попал в беду и просят перевести некоторую сумму денег для решения проблемы.

Стоит выделить такой способ кражи, как фишинг. Это вид мошенничества, целью которого является получение реквизитов карты. Владельцу счета приходит письмо на почту от банка, где его просят перейти по указанной ссылке. При переходе, его может ждать практически идентичный сайт, где пользователя и просят ввести свою конфиденциальную информацию, даже под предлогом простой системной проверки. Распространены так же фишинговые сайты (Аляев, 2010а). Допустим, вы решили слетать отдохнуть. И при поиске выгодного предложения, находите самый достойный вариант. Не думая, вы совершаете

покупку билетов, параллельно собирая чемоданы, но увы, даже спустя три часа, билеты на почту вам так и не приходят.

Поговорим о таком способе, который называется – скримминг. Его название пошло от считывающего переносного устройства, которое мошенники устанавливают на банкоматы. Эти приспособления, созданы для незаконного получения данных банковских карт. Скриммером может является, как специальная накладка, прилепляемая к картридеру, так и миниатюрная видеокамера, направленная на клавиатуру. Широко распространены специальные накладки на клавиатуру, считывающие ПИН-код. Такие устройства крепятся к банкомату на самый обычный двусторонний скотч. После того, как все нужные данные получены, изготавливается копия карты, по которой можно спокойно снимать денежные средства (Katorin, 2016).

Еще об одном интересном виде мошенничества рассказали в обзоре Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) за 2018 год. Он основан на “несовершенстве сценариев обработки переводов с карты на карту с использованием банкоматов”. В банкомате, мошенник выбирает P2P перевод (от клиента к клиенту) и вводит номер карты получателя. Далее, банк одновременно отправляет два авторизованных сообщения: банку-получатели и банку-отправителю. В случае, если операция может быть одобрена, клиенту практически одновременно приходит одобрение от обоих банков. Выполняется фактический перевод, когда сумма на карте получателя увеличивается и вместе с этим, на карте отправителя замораживается такая же сумма. После того, как отправитель не соглашается на списание комиссионных за операцию, банк инициировавший операцию, сообщает банку-получателю и банку-отправителю о возврате. Замороженные средства на карте отправителя размораживаются, но получатель уже снял отправленные ему средства (ФинЦЕРТ, 2018а).

4. Результаты

На мой взгляд, основная проблема заключается в финансовой грамотности. В 2018 году аналитический центр НАФИ, провели исследование на тему финансовой грамотности, путем опроса. Из максимально возможных 21 балла, индекс финансовой грамотности россиян составляет 12,1 балл. Так же выяснили, что финансовая грамотность нелинейно связана с возрастом человека. Примерно до 30 лет происходит накопление знаний и достигает показателя 12,5, и уже после 45 лет начинает снижаться (НАФИ).

Мне кажется, обучать распоряжаться финансами нужно еще со школы. Ведь, чем больше ты вовлечен в финансовую активность, тем быстрее ты накопишь нужный опыт, а соответственно будешь больше знать о безопасности.

Свою первую пластиковую карту я получил в 14 лет. И даже не думал о том, что с куска пластика, можно украсть деньги. В банке мне так же не рассказали о том, что существует, множество способов кражи. Все что я знал тогда, что есть ПИН-код, который нельзя сообщать посторонним людям. Но меня никто не предупредил, что так же нельзя сообщать остальные реквизиты и особенно по телефонному разговору якобы сотрудникам банка. В 14 лет мошенничество меня, конечно, обошло стороной, да и если бы пытались, то списывать там было нечего. Но сколько еще таких же людей, которых банально, не спешат вводить в курс дела даже сотрудники банка.

Банки решили бороться с воровством, путем приостановки подозрительных операций. В сентябре 2018 года ЦБ РФ привел 3 признака подозрительной активности (Приказ Банка России…):

1. Получатель средств числится в базе данных попыток перевода денежных средств без согласия клиента.
2. Устройства с которого осуществляется перевод, совпадает с устройством, внесенным в соответствующую базу.
3. Несоответствие характера, параметров, объема обычным операция клиента.

Так же, сами банки, через мобильное приложение, проводят профилактику и предупреждают об основных видах мошенничества, простым языком, что повышает вероятность прочтения (https://stopfraud.rocketbank.ru/)

5. Заключение

Практически всех вышеописанных уловок можно избежать, если соблюдать одно простое правило: никому и никогда не сообщать реквизиты банковской карты (Памятка...). Никогда работник банка, не будет опекать вас лично и звонить, чтобы сообщить о подозрительных операциях. Ни один работник банка, не будет просить клиента, сообщить проверочный код из СМС и тем более не станет просить назвать ПИН-код вашей карты, ведь не зря ПИН-конверты делают таким образом, чтобы обеспечить невозможность просмотра данных, пока он запечатан. И многие банки уже отказались от таких конвертов, чтобы клиент сам придумал ПИН-код. Работники банка, всегда говорят, что данные карты никому нельзя сообщать, но я ни разу не слышал, чтобы они предупреждали клиентов о том, что сотрудники банка никогда сами не звонят, что было бы неплохо.

Если вы все-таки потеряли карту, следует сразу ее заблокировать, многие банки сейчас позволяют заблокировать/разблокировать карту через официальное приложение, так что даже не нужно посещать отделение или звонить (Балабанов, 2001; Ивлев, Попова, 2002).

Помните о том, что если карта с поддержкой бесконтактной оплаты, а вы опасаетесь, что можете ее потерять, то стоит отключить эту функцию (о чем сотрудникам банка тоже стоило бы сообщать), это так же можно сделать через официальное приложение или позвонив по горячей линии.

Так же не стоит производить покупки, на непроверенных интернет сайтах. Всегда обращайте внимание на адресную строку (Рисунок 8). Если вы не уверены в том, что способны обеспечить безопасность своих средств, то лучше завести отдельную карту, для оплаты в интернете.

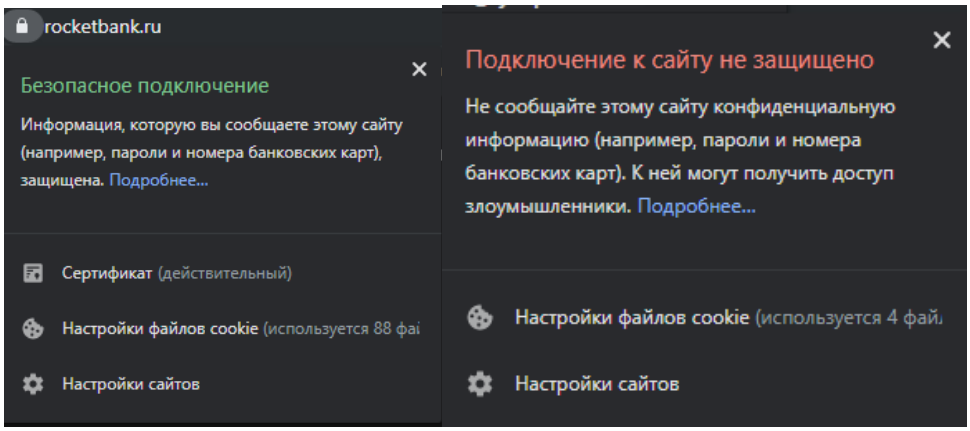

Рис. 8. Безопасное/небезопасное подключение

Всегда осматривайте банкоматы, перед тем как им воспользоваться, а лучше пользоваться теми, которые находятся в отделении банка.

Если карта застряла в банкомате, то сначала заблокируйте ее, перед тем как уйти, чтобы позвать сотрудника.

Никогда не передавайте карту третьим лицам. Даже если в баре, официант хочет уйти с вашей картой для оплаты.

Не оплачивайте покупки, не заходите в банковские приложения с чужих гаджетов.

Если потеряли телефон, то сразу идите в банк и просите отключить карту от потерянного номера и смените логин и пароль для входа в личный кабинет.

Ну и самое главное – это всегда будьте бдительны и перепроверяйте информацию.

Литература

27.мвд.рф – В Хабаровске задержан подозреваемый в серии краж денег с банковских карт [Электронный ресурс]. URL: https://27.xn--b1aew.xn--p1ai/news/item/17025704/ (дата обращения: 14.11.2019).

Аляев, 2010а – *Аляев Д.А.* Актуальные категории карточного мошенничества и механизмы его предотвращения. Социально-экономические проблемы кооперативного

сектора экономики / *Материалы III Международной научно-практической конференции молодых ученых-преподавателей, сотрудников, аспирантов и соискателей*. М.: Российский университет кооперации, 2010. с. 25-28.

Балабанов, 2001 – *Балабанов И.Т.* Электронная коммерция. СПб.: Питер, 2001.

ВЦИОМ – Банковские карты против наличных: выбираем удобство [Электронный ресурс]. URL: https://wciom.ru/index.php?id=236&uid=9581 (дата обращения: 06.11.2019).

Ивлев, Попова, 2002 – *Ивлев В., Попова Т.* Balanced ScoreCard – альтернативные модели // *Банки и технологии*. 2002. №4.

НАФИ – Рейтинг финансовой грамотности регионов России – 2018 [Электронный ресурс]. URL: https://nafi.ru/projects/finansy/reyting-finansovoy-gramotnosti-regionov-rossii-2018/ (дата обращения: 21.11.2019).

Памятка – Памятка «О мерах безопасного использования банковских карт» [Электронный ресурс]. URL: http://www.cbr.ru/content/document/file/16157/sec_card_flyer.pdf (дата обращения: 21.11.2019).

Печникова и др., 2007 – *Печникова А.В., Маркова О.М., Стародубцева Е.Б.* Банковские операции. М.: ИНФРА-М, 2007. 366 с.

Приказ Банка России... – Приказ Банка России от 27 сентября 2018 года № ОД-2525. Признаки осуществления перевода денежных средств без согласия клиента [Электронный ресурс]. URL: https://www.cbr.ru/Content/Document/File/47786/priznaki_20180928.pdf (дата обращения: 21.11.2019).

ФинЦЕРТ, 2018 – ФинЦЕРТ «Обзор несанкционированных переводов денежных средств за 2018 год» [Электронный ресурс]. URL: https://www.cbr.ru/Content/Document/File/62930/ gubzi_18.pdf (дата обращения: 06.11.2019).

ФинЦЕРТ, 2018а – ФинЦЕРТ «Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году» [Электронный ресурс]. URL: http://www.cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf (дата обращения: 14.11.2019).

ЦБ РФ – Количество платежных карт, эмитированных кредитными организациями, по типам карт [Электронный ресурс]. URL: http://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet013.htm (дата обращения: 06.11.2019).

Katorin, 2016 – *Katorin Yu.F.* Bank Cards and the Safety // *Vestnik policii,* 2016, Vol.(9), Is. 3, pp. 121-128.

References

27.mvd.rf – V Khabarovske zaderzhan podozrevaemyi v serii krazh deneg s bankovskikh kart [A suspect in a series of theft of money from bank cards]. [Elektronnyi resurs]. URL: https://27.xn--b1aew.xn--p1ai/news/item/17025704/ (data obrashcheniya: 14.11.2019). [in Russian]

Alyaev, 2010a – *Alyaev D.A.* (2010). Aktual'nye kategorii kartochnogo moshennichestva i mekhanizmy ego predotvrashcheniya. Sotsial'no-ekonomicheskie problemy kooperativnogo sektora ekonomiki [Actual categories of card fraud and mechanisms for its prevention. Socio-economic problems of the cooperative sector of the econom]. *Materialy III Mezhdunarodnoi nauchno-prakticheskoi konferentsii molodykh uchenykh-prepodavatelei, sotrudnikov, aspirantov i soiskatelei.* M.: Rossiiskii universitet kooperatsii, pp. 25-28. [in Russian]

Balabanov, 2001 – *Balabanov I.T.* (2001). Elektronnaya kommertsiya [E-commerce]. SPb.: Piter. [in Russian]

VTsIOM – Bankovskie karty protiv nalichnykh: vybiraem udobstvo [Bank cards versus cash: choose convenience]. [Elektronnyi resurs]. URL: https://wciom.ru/index.php?id=236&uid=9581 (data obrashcheniya: 06.11.2019). [in Russian]

Ivlev, Popova, 2002 – *Ivlev V., Popova T.* (2002). Balanced ScoreCard – al'ternativnye modeli [Balanced ScoreCard – alternative models]. *Banki i tekhnologii.* №4.

NAFI – Reiting finansovoi gramotnosti regionov Rossii – 2018 [Rating of financial literacy of regions of Russia – 2018]. [Elektronnyi resurs]. URL: https://nafi.ru/projects/finansy/reyting-finansovoy-gramotnosti-regionov-rossii-2018/ (data obrashcheniya: 21.11.2019). [in Russian]

Pamyatka – Pamyatka «O merakh bezopasnogo ispol'zovaniya bankovskikh kart» [Memo "On Measures for Safe Use of Bank Cards"]. [Elektronnyi resurs]. URL: http://www.cbr.ru/content/document/file/16157/sec_card_ flyer.pdf (data obrashcheniya: 21.11.2019).

Pechnikova i dr., 2007 – *Pechnikova A.B., Markova O.M., Starodubtseva E.B.* (2007). Bankovskie operatsii [Bank operations]. M.: INFRA-M, 366 p.

Prikaz Banka Rossii... – Prikaz Banka Rossii ot 27 sentyabrya 2018 goda № OD-2525. Priznaki osushchestvleniya perevoda denezhnykh sredstv bez soglasiya klienta [Order of the Bank of Russia dated September 27, 2018 No. OD-2525. Signs of the transfer of funds without the consent of the client]. [Elektronnyi resurs]. URL: https://www.cbr.ru/Content/Document/File/47786/priznaki_20180928.pdf (data obrashcheniya: 21.11.2019).

FinTsERT, 2018 – FinTsERT «Obzor nesanktsionirovannykh perevodov denezhnykh sredstv za 2018 god» [Overview of Unauthorized Money Transfers for 2018]. [Elektronnyi resurs]. URL: https://www.cbr.ru/Content/Document /File/62930/ gubzi_18.pdf (data obrashcheniya: 06.11.2019).

FinTsERT, 2018a – FinTsERT «Obzor osnovnykh tipov komp'yuternykh atak v kreditno-finansovoi sfere v 2018 godu» [Overview of the main types of computer attacks in the credit and financial sphere in 2018]. [Elektronnyi resurs]. URL: http://www.cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf (data obrashcheniya: 14.11.2019).

TsB RF – Kolichestvo platezhnykh kart, emitirovannykh kreditnymi organizatsiyami, po tipam kart [The number of payment cards issued by credit cards, by type of card]. [Elektronnyi resurs]. URL: http://www.cbr.ru/statistics/p_sys/print.aspx? file=sheet013.htm (data obrashcheniya: 06.11.2019). [in Russian]

Katorin, 2016 – *Katorin Yu.F.* (2016). Bank Cards and the Safety. *Vestnik policii.* Vol.(9), Is. 3, pp. 121-128.

Виды мошенничества с банковскими картами и безопасность

Вадим Александрович Смирнов [a, *]

[a] Государственный университет морского и речного флота имени адмирала С.О. Макарова, Российская Федерация

Аннотация. Данная статья посвящена вопросам безопасности при использовании банковских карт и банкоматов, так как проведение денежных операций с использование карт, стало неотъемлемой частью жизни практически каждого человека и из-за неосведомленности и невнимательности людей, мошенники активно этим пользуются. Приводится график выпущенных карт и количество краж с их использованием, а также перечень основных видов краж и новых уловок преступников, для проведения несанкционированных операций. Описаны способы, которые применяют банки, для борьбы с преступностью и что нужно сделать для повышения финансовой грамотности населения. Сделан вывод, что для безопасности своих средств, нужно придерживаться нескольких простых правил и помнить о том, что реквизиты банковских карт нельзя сообщать никому и ни при каких условиях.

Ключевые слова: банковская карта, мошенники, денежные средства, несанкционированная операция, безопасность, банкомат.

* Корреспондирующий автор
Адреса электронной почты: vadimkasmi@mail.ru (В.А. Смирнов)