Команда Центрального федерального округа

«Aerarium sapiens»

Экономический факультет МГУ имени М.В. Ломоносова

Название работы: «Несанкционированное списание денежных средств»

Финансовая грамотность в вузах
ФЕДЕРАЛЬНЫЙ СЕТЕВОЙ МЕТОДИЧЕСКИЙ ЦЕНТР

ОЛИМПИАДА ПО ФИНАНСОВОЙ ГРАМОТНОСТИ

Информация об участниках:

1. Бобровский Алексей Алексеевич – студент Воронежского государственного университета, экономического факультета, кафедра финансов и кредита.
Адрес электронной почты: livenka97@mail.ru

2. Державина Арина Сергеевна - студентка Воронежского государственного университета, экономического факультета, кафедра финансов и кредита.
Адрес электронной почты: ar_derzhavina@mail.ru

3. Шульгина Юлия Игоревна - студентка Воронежского государственного университета, экономического факультета, кафедра финансов и кредита.
Адрес электронной почты: julia_igorevna_2602@mail.ru

4. Пантыкина Юлия Игоревна - студентка Воронежского государственного университета, экономического факультета, кафедра финансов и кредита.
Адрес электронной почты: inp69-12@yandex.ru

5. Дятлова Виктория Александровна - студентка Воронежского государственного университета, экономического факультета, кафедра финансов и кредита.
Адрес электронной почты: viktoriya_dyatlova@mail.ru

Преподаватель – тренер: Бородина Анна Сергеевна.
Основное место работы – Федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный университет».
Адрес электронной почты: borodina_as@list.ru

Воронеж - 2018

Введение

Сегодня почти у каждого совершеннолетнего гражданина Российской Федерации (далее – РФ) есть банковский счет и банковская пластиковая карта, которой удобно оплачивать товары и услуги, в том числе совершая интернет-покупки. Безналичные расчеты, совершаемые посредством пластиковых карт, давно стали целью злоумышленников, и с каждым годом число таких преступлений растет. Поэтому проблема несанкционированного списания денежных средств со счетов клиентов является актуальной для большинства банков. Мошенничество чаще всего осуществляется в результате незаконного вмешательства в применяемые банком технологии обслуживания и расчетов по счетам клиентов, а также хищения персональных данных клиентов банков. Такие преступления снижают доверие граждан к безналичным расчетам, что негативно сказывается на потенциале развития российской экономики. Таким образом, проблема несанкционированного списания денежных средств со счетов клиентов банков, представляется актуальной и требующей комплексного решения.

Целью исследования является разработка рекомендаций по предотвращению несанкционированного списания денежных средств граждан со счетов в банках на основе анализа законодательно-нормативной базы, судебной практики, статистических данных и международного опыта. Для достижения поставленной цели, следует решить следующие задачи:

- представить и проанализировать действующую законодательно-нормативную базу по теме кейса;

- провести анализ статистических данных несанкционированных списаний денежных средств;

- оценить результаты судебной практики в России по теме кейса;

- исследовать международный опыт решения подобных проблем;

- разработать рекомендации по решению проблемы, поставленной в кейсе, ответить на поставленные в кейсе вопросы.

В процессе исследования применялись следующие методы: наблюдение, сравнение, группировка, анализ и синтез, комплексный подход.

Информационную базу исследования составили законодательные и нормативные акты Российской Федерации, материалы судебной практики, научные труды ученых-экономистов, статистические материалы, статьи периодических изданий, ресурсы сети Интернет.

Основные положения работы

Проблема несанкционированного списания денежных средств в современных условиях приобретает важное значение. Мошенники разрабатывают многообразные способы и приемы взлома банковских технологий. В ответ банки стремятся исключить незаконное вмешательство и обезопасить счета и конфиденциальную информацию своих клиентов. Конкретизировать проблему позволяет анализ количества и объема несанкционированных операций (см. Рисунок 1).

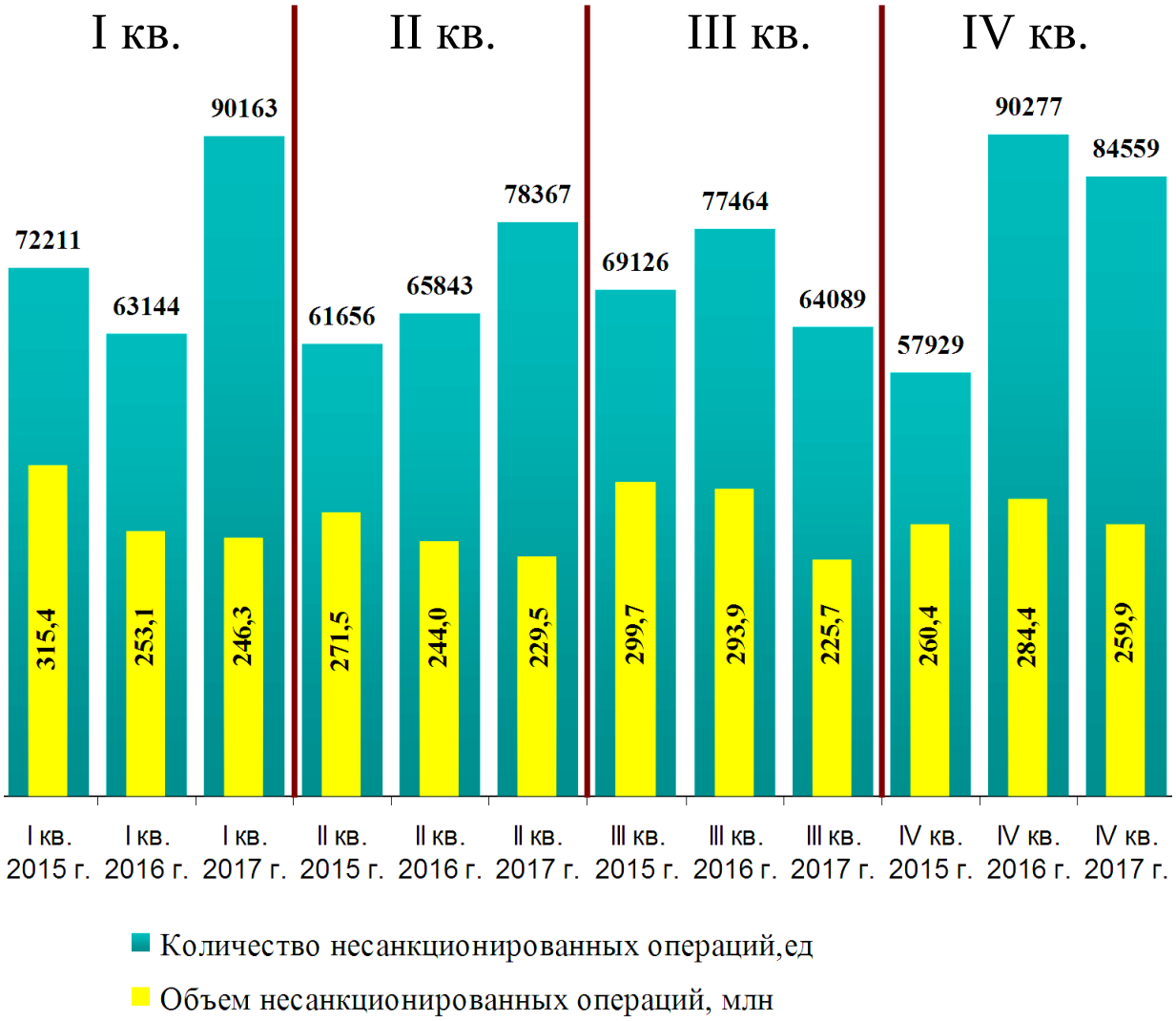


Рисунок 1 - Доля несанкционированных операций с использованием платежных карт в разрезе их объема и количества

Источник: составлено авторами на основе обзора данных Центрального банка РФ о несанкционированных переводов денежных средств за 2015 – 2017 гг.

Данный график иллюстрирует изменение количества несанкционированных операций, а также их объема за 2015 – 2017 гг. в поквартальном разрезе. Согласно анализу представленных данных (см. Приложение 1) наибольшее изменение показателей приходится на

четвертый квартал. Общая тенденция изменения показателей указывает на уменьшения общего объема несанкционированных операций (см. Приложение 2), но количество таких операций увеличивается. Так, за анализируемый период объем снизился на 55,5 млн. руб. или на 17,60%, а количество возросло на 12348 ед. или на 17,39%. Доля объема несанкционированных операций в общем объеме операций (см. Приложение 3), совершенных с использованием платежных карт, в 2017 г. составила 0,0016%, относительно сохраняя нисходящий тренд, при увлечении количества таких операций. Эти значения отражают, в определенной степени, эффективность борьбы с мошенниками и усложнение несанкционированного списания крупных сумм, но их, по нашему мнению, недостаточно для того, чтобы полностью устранить эту проблему. Более того, мошенники постоянно совершенствуют свои приемы и методы взлома, поэтому банкам также следует совершенствовать методы соответствующей защиты, а их клиентам – повышать уровень своей финансовой грамотности, чтобы не попасться на уловки мошенников.

Нормативно-правовое регулирование операций с платежными картами основано на следующих документах: Гражданском кодексе РФ (далее – ГК РФ), который определяет основы договора банковского счета и операций по счету, права распоряжения денежными средствами, находящимися на счете [1]; Уголовном кодексе РФ (далее – УК РФ), где определена ответственность за преступления с использованием платежных карт [2]. В 2011 г. был принят федеральный закон N 161-ФЗ "О национальной платежной системе", который определил основы организации платежных систем, их регулирование, основы регулирования оказания платежных услуг, порядок операций с электронными средствами платежа, а также требования к субъектам национальной платежной системы. Впоследствии закон изменялся и дополнялся. В частности, статья 9, которая полностью вступила в силу 1 января 2014 г., регулирует обязанности оператора по информированию клиента об использовании электронного средства платежа и порядок возмещения суммы операции. Содержание этой статьи предполагает защиту клиентов от мошеннических действий. Однако данный вопрос остается открытым. Банк России не раз давал ответы на вопросы по применению данной статьи. Также защиту от мошенничества должно обеспечивать «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» N 382-П от 9 июня 2012 г., в частности, требования к оператору по защите информации при переводе денежных средств с применением платежных карт, банкоматов и терминалов от несанкционированного доступа, от вредоносных кодов, при использовании сети Интернет.

Основываясь на информации об объеме и количестве несанкционированно списанных денежных средств с платежных карт, можно сделать вывод, что законодательство в полной мере не обеспечивает защиту клиентов от действий мошенников. При этом нельзя исключать человеческий фактор, и, чтобы снизить риски несанкционированного списания средств, Банк России разработал памятку «О мерах безопасного использования банковских карт», которая размещена на официальном сайте учреждения.

Основываясь на законодательстве РФ, справочно-правовая система «Гарант» разработала инфографику "Порядок действий при хищении денег с карты" [11]. Она включает следующие действия при несанкционированном списании денежных средств:

- незамедлительно сообщить о хищении по телефону в банк и потребовать заблокировать карту либо заблокировать карту в личном кабинете самостоятельно;

- заявить о хищении в полицию по телефону или лично;

- не позднее дня, следующего за днем получения от банка уведомления о списании денег, прибыть в отделение банка и подать письменное уведомление о хищении и о блокировке карточного счета.

По мере создания регулятором новых методов борьбы с недобросовестным списанием, эволюционируют и преступные схемы. Так, по данным на 2015 г., проведение транзакций с использованием похищенных карт и PIN-кода составили 63,81% в структуре совершенных преступлений; проведение транзакций с использованием поддельных банковских карт — 4,96%; хищение, сопряженное с несанкционированным внесением изменений в программы — 8,86% и т. д.

С развитием цифровых технологий одним из самых популярных способов хищения денежных средств с карт владельцев стало интернет-хищение. В статистике по типу разделегированных доменов, по данным Банка России, первое место занимают P2P переводы — 23%, страховые компании — 12,3%, а также лжебанки — 12%.

Рисунок 2 – Портрет типичного мошенника

Портрет «типичного» мошенника можно увидеть на рисунке 2. Пол, возраст, профессия и иные качества потерпевшего не имеют существенной роли при проведении анализа, так как практически все жертвы хищений совершают неосмотрительные действия с картой или при использовании интернет-ресурсов.

Обзор судебной практики показывает, что в абсолютном большинстве случаев (в 10 из 11 рассмотренных) суд апелляционной инстанции отказывает истцу (клиенту банка) в удовлетворении требования о взыскании неправомерно списанных денежных средств [4]. Принятие решений в пользу финансово-кредитных организаций обусловлено введением корректных ПИН-кодов и отсутствием фактов компрометации карт. Частичное удовлетворение требования стало возможным, благодаря зафиксированной серии хакерских атак, совершенных на серверы банка. В подобном случае клиенту удастся получить возмещение, так как воровство произошло по вине финансовой организации.

Решение проблемы несанкционированного списания в РФ невозможно без анализа зарубежного опыта. В Приложении 4 представлена информация ресурса The Nilson Report, которая отражает общемировую тенденцию роста убытков от мошеннических операций с кредитными картами. В Приложении 5 представлены данные о доле различных видов списаний в общей структуре на примере США, Франции и Канады. Похищение данных кредитных карт является самым распространенным способом кражи как в России, так и за рубежом, что подтверждает общемировой характер проблемы и требует анализа действующих и разработки потенциально возможных инструментов регулирования несанкционированного списания денежных средств (см. Приложение 6).

Из предложенного перечня инструментов, направленных на предотвращение несанкционированного списания денежных средств, в соответствии с критериями «цена реализации», «скорость внедрения», «величина прогнозируемого эффекта» и «гармонизация интересов участников», нами были выбраны следующие: оповещение клиентов посредством SMS-сообщений и писем электронной почты, технология 3D Secure, биометрическая аутентификация, повышение финансовой грамотности населения.

В целях выявления наиболее эффективного инструмента был проведен опрос среди студентов высшего учебного заведения (150 человек). В ходе анализа полученных данных было выявлено, что 25,83% опрошенных сталкивались с проблемой несанкционированного списания денежных средств (из них 7,50% - неоднократно), среди которых 29,00% самостоятельно разгласили конфиденциальную информацию третьим лицам (см. Рисунок 3). В иных случаях респонденты возлагают ответственность на коммерческие банки (54,10%) и мегарегулятор (12,30%).

Из действующих инструментов борьбы с мошенничеством наибольшим доверием среди всех опрошенных пользуется система подтверждения операций посредством SMS-сообщений (72,50% респондентов).

Из потенциально возможных инструментов борьбы с мошенничеством, с нашей точки зрения, самым эффективным является использование биометрических данных. Подтверждением этого вывода служит заинтересованность 84,17% участников опроса в применении данных технологий.

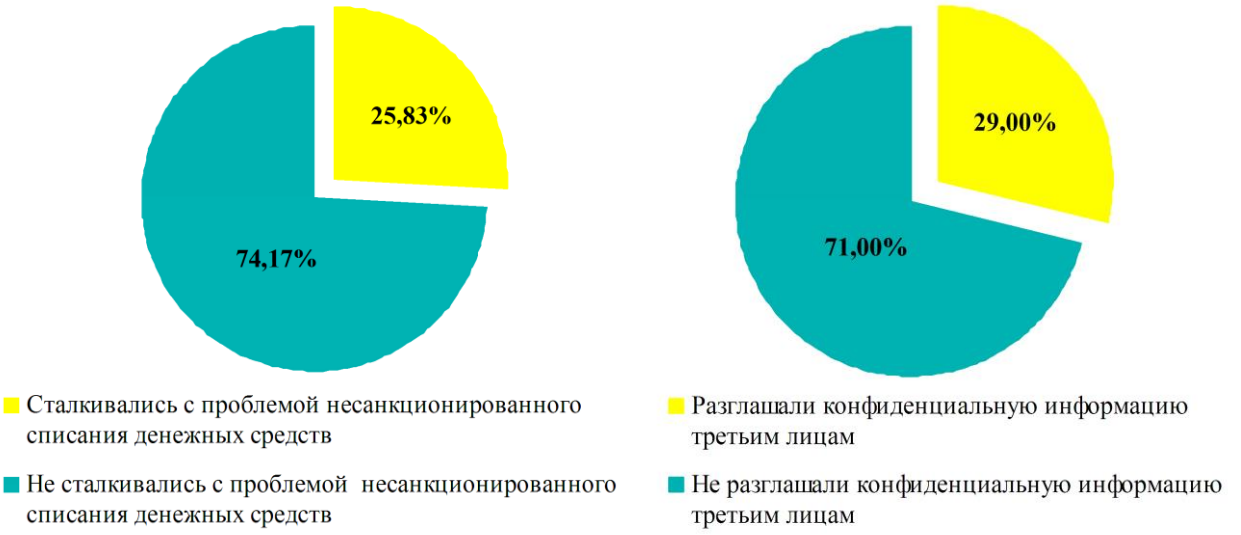


Рисунок 3 - Доли столкнувшихся с проблемой несанкционированного списания денежных средств в целом и по собственной вине.

Источник: составлено авторами на основе данных проведенного опроса.

Очевидно, что для предотвращения несанкционированного списания денежных средств необходимо повышать финансовую грамотность населения. В бланке опроса нами были предложены 4 возможных варианта:

1) обучающие курсы (добровольные);
2) введение в учебных заведениях предмета «Управление личными финансами»;
3) приложения для мобильных и других устройств;
4) издание справочников для самообразования.

Наибольшей популярностью пользуются второй и третий из предложенных вариантов (40,65% и 34,15% соответственно), а самым непопулярным – четвертый (5,70%).

Эти результаты могут послужить ориентиром для деятельности государства в области повышения финансовой грамотности.

Вместе с тем следует учитывать потенциальные риски, способствующие несанкционированному списанию денежных средств:

- обращение обезличенных операторами связи («серых») SIM-карт;

- недостаточная аппаратная и программная защита банкоматов и платежных терминалов.

Ответы на вопросы кейса.

1. К ошибкам героя кейса можно отнести:

- нарушение условий договора обслуживания банковской карты в части конфиденциальности;

- герой не заявил о хищении в правоохранительные органы;

- не установил ежедневный лимит списания;

- не подключил систему оповещения об операциях по карте. (см. Приложение 4).

2. Финансовые институты, с целью снижения риска несанкционированного списания денежных средств со счетов граждан, могут:

- информировать клиентов о порядке действий в случаях несанкционированного списания денежных средств;

- совершенствовать имеющиеся инструменты борьбы с мошенничеством и разрабатывать новые (см. Приложение 6).

3. Регулирующие государственные органы, с целью снижения риска несанкционированного списания денежных средств со счетов граждан, могут:

- внести изменения в ст. 9 федерального закона "О национальной платежной системе", увеличив срок подачи заявления в случае несанкционированного списания денежных средств до трех дней;

- ужесточить меры ответственности лиц, совершивших подобные преступления;

- расширить программы по повышению финансовой грамотности населения;

- создать механизм досудебного урегулирования подобных споров;

- создать рейтинговую систему оценки банков клиентами (см. Приложение 6).

Заключение

В результате проведенного исследования получены следующие выводы.

В процессе совершенствования законодательно-нормативной базы России решено немало вопросов, связанных с несанкционированным списанием денежных средств со счетов клиентов банков, но анализ статистических данных говорит о недостаточности этих преобразований.

Нормативно-правовое регулирование операций с платежными картами основывается на ГК РФ и УК РФ. Также существуют специализированный Федеральный закон N 161-ФЗ "О национальной платежной системе" и Положения Банка России, в которых обозначены требования и нормы по обеспечению защиты информации при осуществлении переводов денежных средств.

Обзор судебной практики показывает, что в абсолютном большинстве случаев (в 10 из 11 рассмотренных) суд апелляционной инстанции отказывает истцу (клиенту банка) в удовлетворении требования о взыскании неправомерно списанных денежных средств.

Анализ международной практики демонстрируют тенденцию роста убытков от мошеннических операций с кредитными картами, что определяет всемирный характер проблемы, а исследование зарубежных методов борьбы с недобросовестными списаниями дало толчок для новых идей банковских инструментов.

Основная причина несанкционированного списания денежных средств — плохая осведомленность населения и уязвимость банковских технологий перед незаконным вмешательством со стороны мошенников. Необходимо, чтобы банки тщательнее отбирали своих сотрудников и регулярно проводили обучение персонала. Второй причиной успеха целевых атак является излишняя вера финансово-кредитных учреждений в то, что стандартные средства защиты, такие как лицензионный и обновленный антивирус, остановят злоумышленников на одном из этапов развития атаки.

Однозначной гарантии защиты от целевых атак на банки не существует, но снизить риски и повысить эффективность защиты банков вполне возможно. Лучше всего это можно сделать с помощью систем сбора, мониторинга и анализа информации об актуальных угрозах, преступных группах, их тактике, инструментах. Необходимо повышать уровень защиты персональных данных владельцев банковских карт. Своевременное распознавание тактики и механизма несанкционированного списания позволяет вовремя закрыть атакующим доступ. Быть на шаг впереди хакеров - значит сохранить свои деньги.

Список использованных источников

1. Гражданский кодекс Российской Федерации. Части первая, вторая, третья и четвертая: текст с изменениями и дополнениями на 21 января 2018 г. – М.: Эксмо, 2018. – 576 с.
2. Уголовный кодекс Российской Федерации: текст с изм. и доп. на 21 января 2018 г. . – М.: Эксмо, 2018. – 224 с.
3. Федеральный закон "О национальной платежной системе" от 27.06.2011 N 161-ФЗ // [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_115625/
4. Апелляционное определение Санкт-Петербургского городского суда от 28.11.2017 N 33-25744/2017 по делу N 2-2905/2017; Апелляционное определение Красно-дарского краевого суда от 18.07.2017 по делу N 33-19614/2017; Апелляционное определе-ние Московского городского суда от 14.07.2017 по делу N 33-27550/2017; Апелляционное определение Санкт-Петербургского городского суда от 23.05.2017 N 33-8704/2017 по делу N 2-1361/2016; Апелляционное определение Московского городского суда от 20.04.2017 по делу N 33-15004/2017; Апелляционное определение Московского городского суда от 18.07.2017 по делу N 33-27910/2017; Апелляционное определение Московского городского суда от 18.07.2017 по делу N 33-27909/2017; Апелляционное определение Московского городского суда от 28.03.2017 по делу N 33-7594/2017; Апелляционное определение Московского городского суда от 06.03.2017 по делу N 33-8075/2017; Апелляционное определение Московского городского суда от 12.07.2017 по делу N 33-27157/2017; Апелляционное определение Московского городского суда от 12.07.2017 по делу N 33-27009/2017
5. Имаева Ю. Б. Особенности расследования хищений, совершенных с использованием кредитных и расчетных карт : автореферат дис. ... кандидата юридических наук : 12.00.12 / Имаева Юлия Борисовна; [Место защиты: Рост. юрид. ин-т МВД РФ]. - Ростов-на-Дону, 2015. - 30 с.
6. Климов А. В. Модели и алгоритмы поддержки управления комплексной безопасностью объектов дистанционного банковского обслуживания населения : автореферат дис. ... кандидата технических наук : 05.13.10 / Климов Александр Валентинович; [Место защиты: Акад. гос. противопожарной службы МЧС России]. - Москва, 2016. - 24 с.
7. Обзор несанкционированных переводов денежных средств за 2017 год. [Электронный ресурс] URL: http://www.cbr.ru/statichtml/file/14435/survey_transfers_17.pdf
8. Обзор несанкционированных переводов денежных средств за 2016 год. [Электронный ресурс] URL: https://www.cbr.ru/statichtml/file/14435/survey_transfers_16.pdf
9. Обзор несанкционированных переводов денежных средств за 2015 год. [Электронный ресурс] URL: http://www.cbr.ru/collection/collection/file/262/survey_2015.pdf

10. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере главного управления безопасности и защиты информации банка России. [Электронный ресурс] URL: http://www.cbr.ru/statichtml/file/14435/gubzi-4.pdf
11. Порядок действий при хищении денег с карты. [Электронный ресурс] URL: http://www.garant.ru/infografika/654413/
12. Страховка от списания. [Электронный ресурс] URL: https://www.rbc.ru/society/14/07/2015/56bcba1f9a7947299f72bdf1
13. Схемы финансового мошенничества: предупрежден, значит защищен. [Электронный ресурс] URL: http://fingramota.zapravazaemschikov.ru/pres/skhemyfinansovogomoshennichestvapreduprezhden-znachit-zashchishchen.pdf
14. Nilson Report [Электронный ресурс] URL: https://nilsonreport.com/upload/content_promo/The_Nilson_Report_Issue_1118.pdf
15. Payments cards and mobile [Электронный ресурс] URL: https://www.paymentscardsandmobile.com/wpcontent/uploads/2015/03/PCM_Alaric_Fraud-Report_2015.pdf
16. Forbes [Электронный ресурс] URL: https://www.forbes.com/sites/johnnyjet/2018/01/30/6-tips-to-help-avoid-card-skimming-at-atms-while-traveling/#1d445bfb2992
17. Forbes [Электронный ресурс] URL: http://www.forbes.ru/finansy-i-investicii/346943-bezopasnost-v-internete-kak-zashchitit-svoi-platezhi

Приложение 1

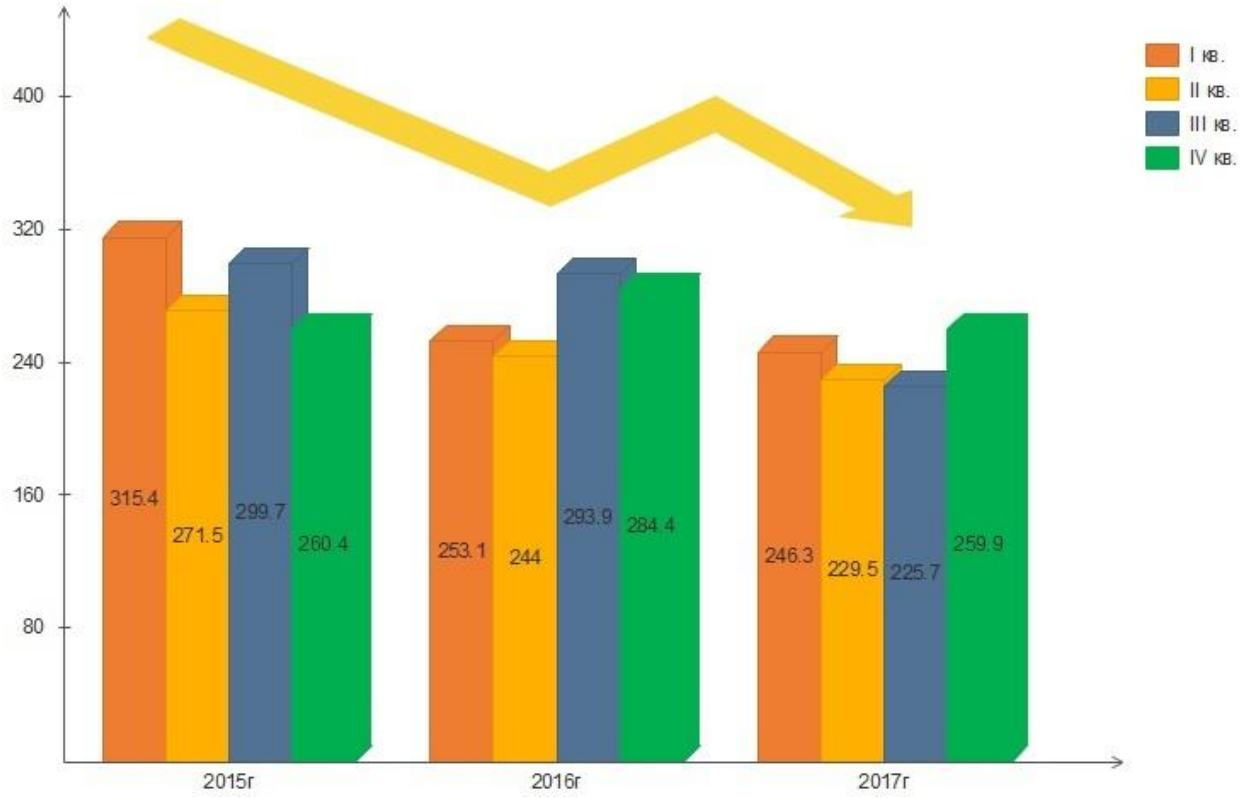
Анализ количества и объема несанкционированных операций с использованием платежных карт за 2015 – 2017 гг. в поквартальном разрезе

Период	Количество несанкционированных операций, ед	Объем несанкционированных операций, млн. руб.	Изменение количества		Изменение объема	
			Абсолютное изменение, ед	Относительное изменение, %	Абсолютное изменение, млн. руб.	Относительное изменение, %
I кв. 2015 г.	72211	315,4	–	–	–	–
I кв. 2016 г.	63144	253,1	-9067	-12,56	-62,3	-19,75
I кв. 2017 г.	90163	246,3	+27019	+42,79	-6,8	-2,69
II кв. 2015 г.	61656	271,5	–	–	–	–
II кв. 2016 г.	65843	244,0	+4187	+6,79	-27,5	-10,13
II кв. 2017 г.	78367	229,5	+12524	+19,02	-14,5	-5,94
III кв. 2015 г.	69126	299,7	–	–	–	–
III кв. 2016 г.	77464	293,9	+8338	+12,06	-5,8	-1,94
III кв. 2017 г.	64089	225,7	-13375	-17,27	-68,2	-23,21
IV кв. 2015 г.	57929	260,4	–	–	–	–
IV кв. 2016 г.	90277	284,4	+32348	+55,84	+24,0	+9,22
IV кв. 2017 г.	84559	259,9	-5718	-6,34	-24,5	-8,61

Источник: составлено авторами на основе данных обзора несанкционированных переводов денежных средств за 2015 – 2017 гг. от Центрального банка Российской Федерации.

Приложение 2

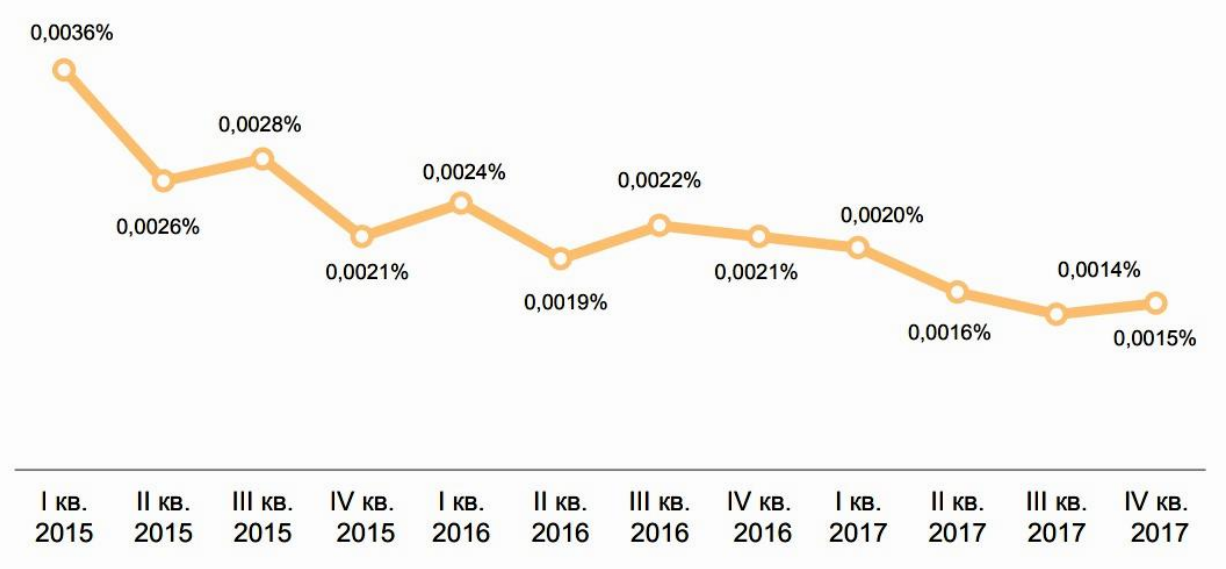
Объем несанкционированных операций за 2015 – 2017 гг., млн руб.



Источник: составлено авторами на основе данных обзора несанкционированных переводов денежных средств за 2015 – 2017 гг. от Центрального банка Российской Федерации.

Приложение 3

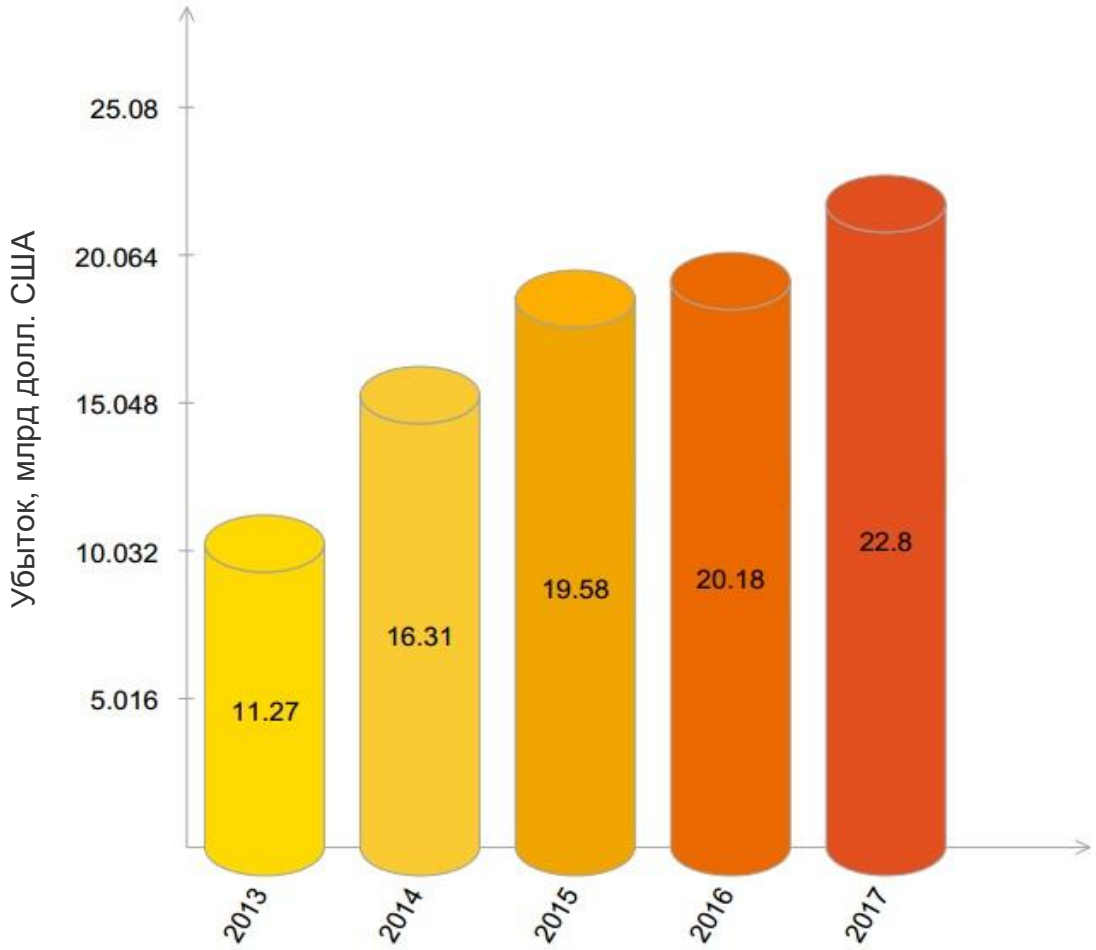
Доля несанкционированных операций с использованием платежных карт в разрезе их объема за 2015 – 2017 гг.



Источник: «Обзор несанкционированных переводов денежных средств за 2017 год от Центрального банка Российской Федерации» (http://www.cbr.ru/statichtml/file/14435/survey_transfers_17.pdf)

Приложение 4

Общемировые убытки от мошеннических операций с кредитными картами



Источник: составлено авторами на основе данных The Nilson Report – информационный ресурс новостей и анализа мировой индустрии платежных карт. (https://www.nilsonreport.com/index.php)

Приложение 5

Структура мошеннических операций с кредитными картами на примере Канады, США и Франции.

Вид операции	Канада	США	Франция
Кража карты	5,4%	18,0%	35,0%
Подделка карты	24,0%	33,0%	0,2%
Кража данных карты	64,4%	42,0%	64,7%
Смена аккаунта и прочее	6,2%	7,0%	0,1%

Источник: составлено авторами на основе данных Payments cards and mobile (https://www.paymentscardsandmobile.com/wp-content/uploads/2015/03/PCM_Alaric_Fraud-Report_2015.pdf)

Приложение 6

Анализ действующих и потенциально возможных инструментов регулирования проблемы несанкционированного списания денежных средств

Название	Описание	Преимущества	Недостатки
1	2	3	4
Основные действующие инструменты урегулирования проблемы			
Оповещения клиентов	Дистанционное оповещение клиентов банков (SMS-сообщения и письма электронной почты)	1. Позволяет предотвратить несанкционированные действия. 2. Позволяет своевременно отозвать ошибочные платежные документы. 3. Позволяет получать оперативную информацию о операциях по счету. 4. Не требует установки сложного программного обеспечения.	1. Пробелы в покрытии сотовых сетей. 2. Относительно высокие затраты. 3. Недостаточная защищенность персональных данных.
Страхование карты	Страхование денежных интересов пользователя карты	1. Возмещение застрахованной суммы клиенту. 2. Повышение доверия клиента. 3. Привлекательно для банков.	Высокие издержки (страховые взносы)
Технология 3D Secure	Протокол защиты, используемый для авторизации держателя карты во время совершения платежной операции посредством сети Интернет.	1. Персональные данные клиента, оставаясь на сервере банка, не попадают в интернет-магазины.	1. Одноразовый пароль может быть украден и перенаправлен. 2. Система используется отдельными интернет-магазинами.
Наличие антивирусной программы	Программное обеспечение для обнаружения вредоносных программ и восстановления заражённых такими программами файлов.	1. Высокая скорость работы. 2. Блокировка fishing-сайтов, шпионских программ и потенциально опасной рекламы. 3. Прост в использовании.	1. Относительно высокая стоимость. 2. Игнорирование некоторых вредоносных программ. 3. Не обязательны к установке.

1	2	3	4
Потенциально возможные направления урегулирования проблемы			
Биометрическая аутентификация	Удостоверение личности пользователя на основе его биометрических данных (сетчатка глаза, отпечатки пальцев, термограмма лица и др.)	1. Трудность фальсификации признаков клиента. 2. Высокая достоверность аутентификации из-за уникальности таких признаков. 3. Неотделимость биометрических признаков от личности пользователя.	1. Высокие издержки. 2. Технические ошибки. 3. Риск увечий клиента. 4. Возможность утечки персональных данных.
Повышение финансовой грамотности населения	Мероприятия по информированию населения о возможных способах совершения несанкционированных операций с использованием платежных карт и мерах защиты.	1. Получение пользователями знаний о видах мошенничества и методах безопасного использования карты. 2. Повышение бдительности потребителей банковских услуг. 3. Повышение доверия к безналичным расчетам и банковской системе в целом.	Дополнительные финансовые издержки банка.
Программы идентификации сомнительных операций	Программное обеспечение, выявляющее на основе определенных критериев, сомнительные операции. Критерии: неоднократное появление у банкоматов безработных; необоснованная поспешность в проведении операции; осуществление расчетов с использованием расчетных счетов третьих лиц и т.д.	1. Сокращение числа операций несанкционированного списания денежных средств. 2. Блокировка счетов, на которые переведены средства по сомнительным операциям на 2 рабочих дня или до выяснения обстоятельств.	Дополнительные финансовые издержки банка.
Рейтинг банков по проценту возврата несанкционированных списаний.	Рейтинг выстраивается на основе отзывов и голосов реальных пользователей (прошедших регистрацию по паспортным данным), которым коммерческие банки вернули/не вернули похищенные средства. Пользователь сможет выбрать причину списания из ряда указанных, основание отказа в возврате денежных средств, либо описать свой вариант случившейся ситуации.	1. Открытый доступ к просмотру; 2. Улучшение имиджа банка в целом; 3. Простота в применении; 4. Представляет собой независимую и относительно надежную оценку; 5. Позволяет клиенту выбрать наиболее надежный банк.	1. Возможна потеря клиентов. 2. Риск фальсификации данных и клеветы в адрес банка

Источник: составлено авторами