

Команда центрального федерального округа под названием



«Aerarium sapiens»



Название работы: «Несанкционированное списание
денежных средств»

Информация об участниках:

1. Бобровский Алексей Алексеевич – студент Воронежского государственного университета, экономического факультета, кафедры финансов и кредита.

Адрес электронной почты: livenka97@mail.ru

2. Державина Арина Сергеевна - студентка Воронежского государственного университета, экономического факультета, кафедры финансов и кредита.

Адрес электронной почты: ar_derzhavina@mail.ru

3. Шульгина Юлия Игоревна - студентка Воронежского государственного университета, экономического факультета, кафедры финансов и кредита.

Адрес электронной почты: julia_igorevna_2602@mail.ru

4. Пантыкина Юлия Игоревна - студентка Воронежского государственного университета, экономического факультета, кафедры финансов и кредита.

Адрес электронной почты: inp69-12@yandex.ru

5. Дятлова Виктория Александровна - студентка Воронежского государственного университета, экономического факультета, кафедры финансов и кредита.

Адрес электронной почты: viktoriya_dyatlova@mail.ru

Преподаватель – тренер: к.э.н. доцент Бородина Анна Сергеевна.

Основное место работы – Федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный университет», кафедра «Финансы и кредит»

Адрес электронной почты: borodina_as@list.ru



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 работы 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;
- 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 научные труды ученых-экономистов, законодательные и нормативные акты Российской Федерации, материалы судебной практики, статистические материалы, статьи периодических изданий, ресурсы сети Интернет.

Основные положения работы

Проблема несанкционированного списания денежных средств имеет широкое распространение. Мошенники создают 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).

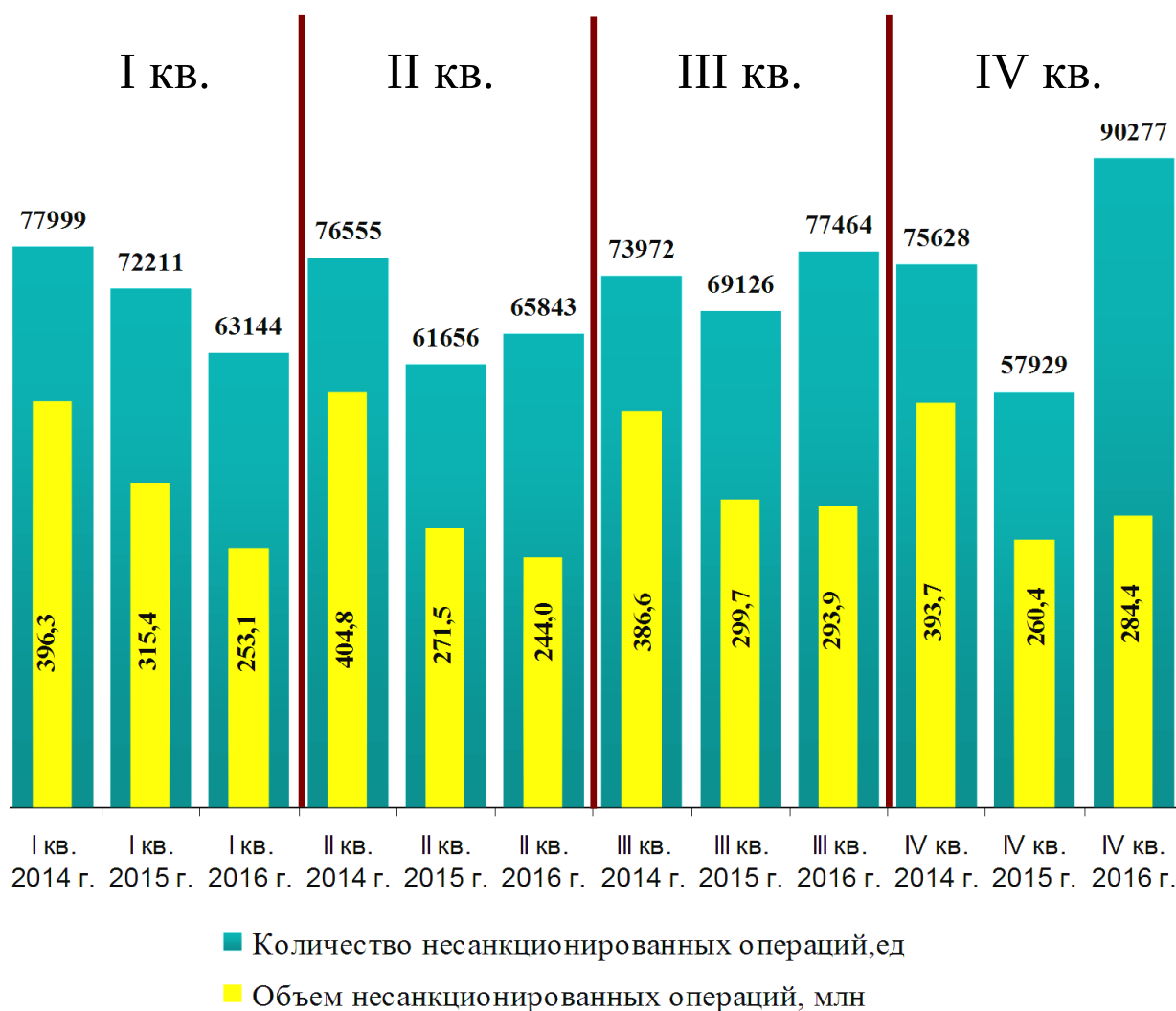


Рисунок 1 - Доля несанкционированных операций с использованием платежных карт в разрезе их объема и количества

Источник: составлено авторами на основе данных обзора несанкционированных переводов денежных средств за 2014 – 2016 гг. от Центрального банка Российской Федерации.

Данный график интерпретирует изменение количества несанкционированных операций, а также их объем за 2014 – 2016 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) и увеличение количества таких операций. За анализируемый период объем снизился на 111,9 млн. руб. или на 28,2%, а количество возросло на 12278 ед. или на 15,7%. Эти значения отражают эффективность борьбы с мошенниками и усложнение несанкционированного списания крупных сумм, но их недостаточно для того, чтобы полностью устранить эту проблему, более того, мошенники постоянно совершенствуют свои приемы и методы взлома, поэтому банкам также следует совершенствовать свои методы защиты, а их клиентам повышать уровень своей финансовой грамотности, чтобы не попасться на уловки мошенников.

Анализ доли несанкционированных операции с использованием платежных карт в общем объеме и количестве операций (см. Приложение 3) подтверждает уменьшение объема, а также снижение их количества, несмотря на рост их абсолютных значений. Это связано, прежде всего, с ежегодным ростом безналичных расчетов.

Нормативно-правовое регулирование операций с платежными картами основывается на Гражданский кодекс РФ (далее – ГК РФ), который определяет основы договора банковского счета, операций по счету, определяет права распоряжения денежными средствами на счете [1]. В Уголовном кодексе РФ (далее – УК РФ) 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» (см. Приложение 4).

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 делегированных доменов, по данным Банка России, первое место занимают P2P переводы — 23%, страховые компании — 12,3%, а также лжебанки — 12%.

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.



Рисунок 2 – Портрет типичного мошенника

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.

Для анализа проблемы недобросовестных списаний следует обратиться к данным зарубежной статистики. В Приложении 5 представлена информация ресурса The Nilson Report, которая отражает общемировую тенденцию роста убытков от мошеннических операций с кредитными картами. В Приложении 6 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 проблемы несанкционированного списания денежных средств (см. таблицу 1).

Таблица 1 – 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)

Продолжение таблицы 1

1	2	3	4
Технология 3-D 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.
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.

Продолжение таблицы 1

1	2	3	4
---	---	---	---

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

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. таблицу 1).

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. таблицу 1).

Заключение

В результате проведенного исследования получены следующие выводы и результаты.

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, 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 определение 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 2016 год. [Электронный ресурс] URL: https://www.cbr.ru/statichtml/file/14435/survey_transfers_16.pdf
8. Обзор несанкционированных переводов денежных средств за 2015 год. [Электронный ресурс] URL: http://www.cbr.ru/collection/collection/file/262/survey_2015.pdf
9. Обзор несанкционированных переводов денежных средств за 2014 год. [Электронный ресурс] URL: http://www.cbr.ru/collection/collection/file/263/survey_2014.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.zpravazaemschikov.ru/pres/skhemyfinansovogomoshennichestvapreduprezhd-en-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.paymentscardsand-mobile.com/wpcontent/uploads/2015/03/PCM_Alarc_Fraud-Report_2015.pdf
16. Forbes [Электронный ресурс] URL: <https://www.forbes.com/sites/john-nyjet/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-svoiplatezhi>

Приложение 1

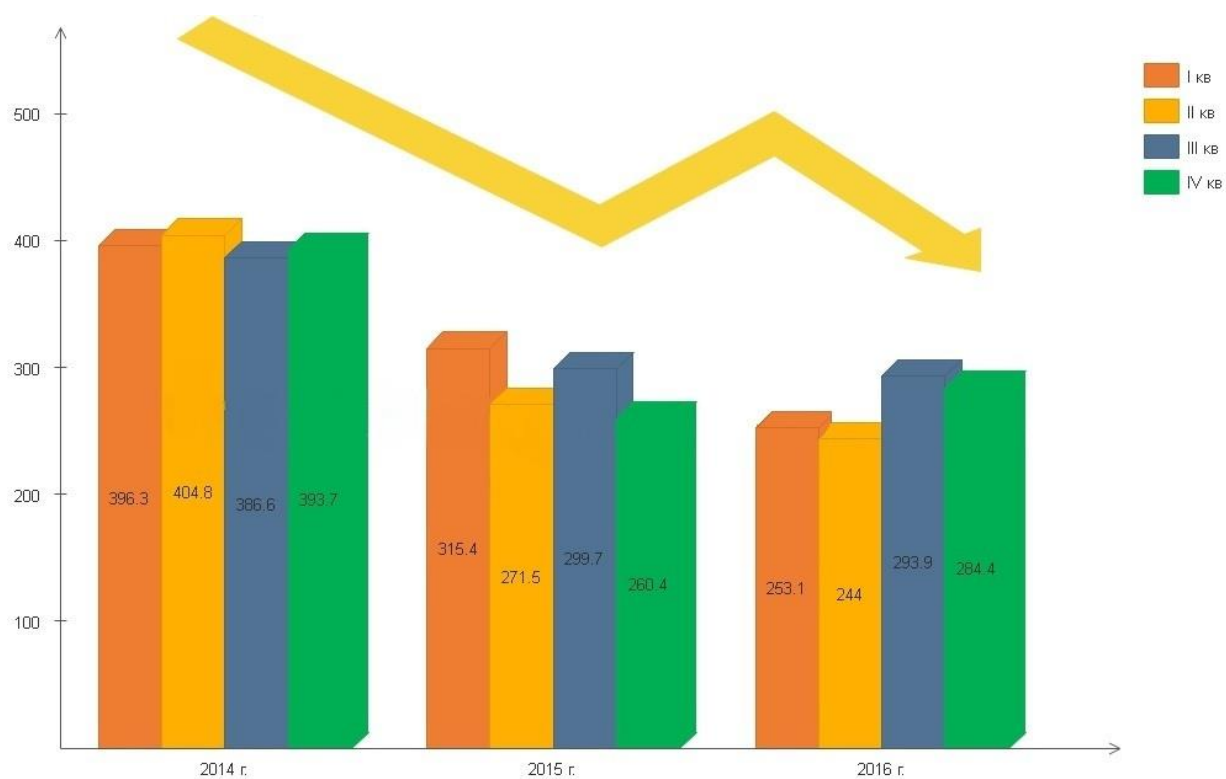
Анализ количества и объема несанкционированных операций с использованием платежных карт за 2014 – 2016 гг. в поквартальном разрезе

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. 2014 г.	77999	396,3	–	–	–	–
I кв. 2015 г.	72211	315,4	-5788	-7,42	-80,9	-20,41
I кв. 2016 г.	63144	253,1	-9067	-12,56	-62,3	-19,75
II кв. 2014 г.	76555	404,8	–	–	–	–
II кв. 2015 г.	61656	271,5	-14899	-19,46	-133,3	-32,93
II кв. 2016 г.	65843	244,0	4187	6,79	-27,5	-10,13
III кв. 2014 г.	73972	386,6	–	–	–	–
III кв. 2015 г.	69126	299,7	-4846	-6,55	-86,9	-22,48
III кв. 2016 г.	77464	293,9	8338	12,06	-5,8	-1,94
IV кв. 2014 г.	75628	393,7	–	–	–	–
IV кв. 2015 г.	57929	260,4	-17699	-23,40	-133,3	-33,86
IV кв. 2016 г.	90277	284,4	32348	55,84	24,0	9,22

Источник: составлено авторами на основе данных обзора несанкционированных переводов денежных средств за 2014 – 2016 гг. от Центрального банка Российской Федерации.

Приложение 2

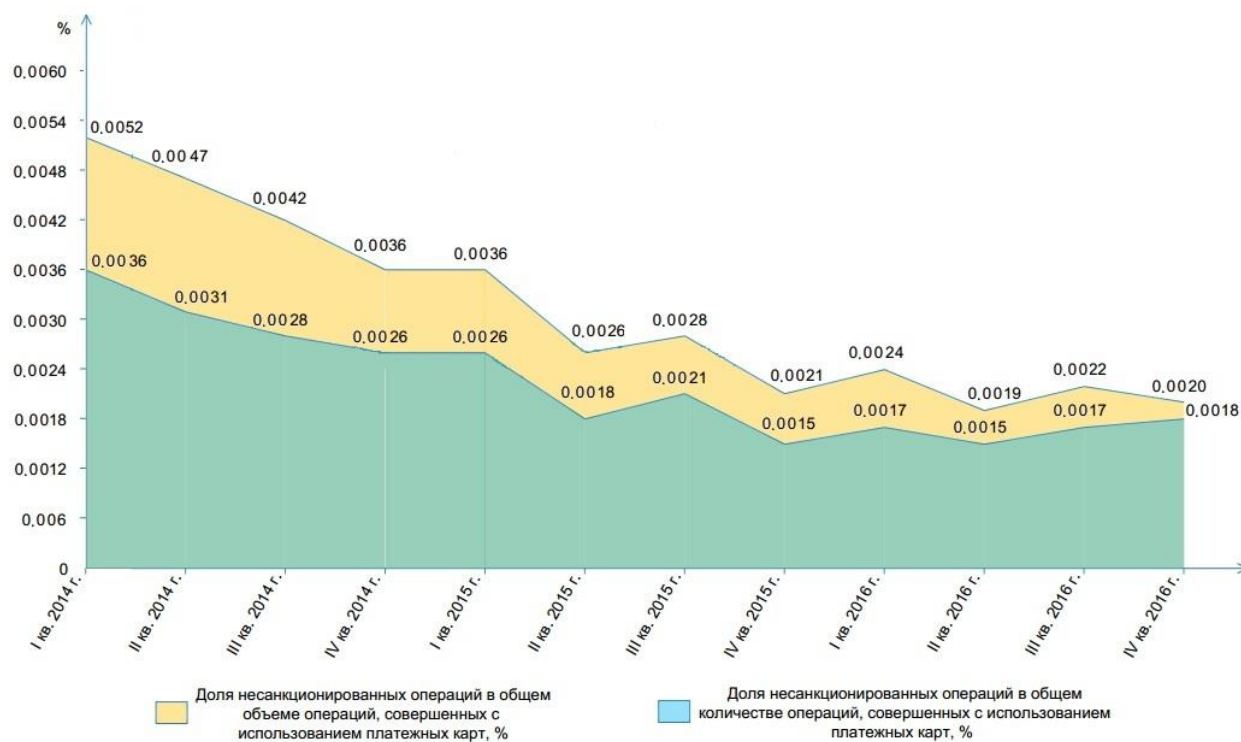
Объем несанкционированных операций за 2014 – 2016 гг., млн руб.



Источник: составлено авторами на основе данных обзора несанкционированных переводов денежных средств за 2014 – 2016 гг. от Центрального банка Российской Федерации.

Приложение 3

Доля несанкционированных операций с использованием платежных карт в общем объеме и количестве операций за 2014 – 2016 гг.



Источник: составлено авторами на основе данных обзора несанкционированных переводов денежных средств за 2014 – 2016 гг. от Центрального банка Российской Федерации.

Приложение 4

Приложение к письму Банка России от 02.10.2009 N 120-Т

ПАМЯТКА «О МЕРАХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ»

Соблюдение рекомендаций, содержащихся в Памятке, позволит обеспечить максимальную сохранность банковской карты, ее реквизитов, ПИН и других данных, а также снизить возможные риски при совершении операций с использованием банковской карты в банкомате, при безналичной оплате товаров и услуг, в том числе через сеть Интернет.

Общие рекомендации.

1. Никогда не сообщайте ПИН третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим Вам в использовании банковской карты.

2. ПИН необходимо запомнить или в случае, если это является затруднительным, хранить его отдельно от банковской карты в неявном виде и недоступном для третьих лиц, в том числе родственников, месте.

3. Никогда ни при каких обстоятельствах не передавайте банковскую карту для использования третьим лицам, в том числе родственникам. Если на банковской карте нанесены фамилия и имя физического лица, то только это физическое лицо имеет право использовать банковскую карту.

4. При получении банковской карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя банковской карты, если это предусмотрено. Это снизит риск использования банковской карты без Вашего согласия в случае ее утраты.

5. Будьте внимательны к условиям хранения и использования банковской карты. Не подвергайте банковскую карту механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Банковскую карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.

6. Телефон кредитной организации - эмитента банковской карты (кредитной организации, выдавшей банковскую карту) указан на оборотной стороне банковской карты. Также необходимо всегда иметь при себе контактные телефоны кредитной организации - эмитента банковской карты и номер банковской карты на других носителях информации: в записной книжке, мобильном телефоне и/или других носителях информации, но не рядом с записью о ПИН.

7. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета целесообразно установить суточный лимит на сумму

операций по банковской карте и одновременно подключить электронную услугу оповещения о проведенных операциях (например, оповещение посредством SMS-сообщений или иным способом).

8. При получении просьбы, в том числе со стороны сотрудника кредитной организации, сообщить персональные данные или информацию о банковской карте (в том числе ПИН) не сообщайте их. Позвоните в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту) и сообщите о данном факте.

9. Не рекомендуется отвечать на электронные письма, в которых от имени кредитной организации (в том числе кредитной организации - эмитента банковской карты (кредитной организации, выдавшей банковскую карту)) предлагается предоставить персональные данные. Не следуйте по "ссылкам", указанным в письмах (включая ссылки на сайт кредитной организации), т.к. они могут вести на сайты-двойники.

10. В целях информационного взаимодействия с кредитной организацией - эмитентом банковской карты (кредитной организации, выдавшей банковскую карту) рекомендуется использовать только реквизиты средств связи (мобильных и стационарных телефонов, факсов, интерактивных web-сайтов/порталов, обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в кредитной организации - эмитенте банковской карты.

11. Помните, что в случае раскрытия ПИН, персональных данных, утраты банковской карты существует риск совершения правонарушений с денежными средствами на Вашем банковском счете со стороны третьих лиц. В случае если имеются предположения о раскрытии ПИН, персональных данных, позволяющих совершить правонарушения с Вашим банковским счетом, а также если банковская карта была утрачена, необходимо немедленно обратиться в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту) и следовать указаниям сотрудника данной кредитной организации. До момента обращения в кредитную организацию - эмитент банковской карты Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета. Как правило, согласно условиям договора с кредитной организацией - эмитентом банковской карты денежные средства, списанные с Вашего банковского счета в результате несанкционированного использования Вашей банковской карты до момента уведомления об этом кредитной организации - эмитента банковской карты, не возмещаются.

Рекомендации при совершении операций с банковской картой в банкомате.

1. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).

2. Не используйте устройства, которые требуют ввода ПИН для доступа в помещение, где расположен банкомат.

3. В случае если поблизости от банкомата находятся посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом.

4. Перед использованием банкомата осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры набора ПИН). В указанном случае воздержитесь от использования такого банкомата.

5. В случае если клавиатура или место для приема карт банкомата оборудованы дополнительными устройствами, не соответствующими его конструкции, воздержитесь от использования банковской карты в данном банкомате и сообщите о своих подозрениях сотрудникам кредитной организации по телефону, указанному на банкомате.

6. Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.

7. Набирайте ПИН таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН прикрывайте клавиатуру рукой.

8. В случае если банкомат работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого банкомата, отменить текущую операцию, нажав на клавиатуре кнопку "Отмена", и дождаться возврата банковской карты.

9. После получения наличных денежных средств в банкомате следует пересчитать банкноты поштучно, убедиться в том, что банковская карта была возвращена банкоматом, дождаться выдачи квитанции при ее запросе, затем положить их в сумку (кошелек, карман) и только после этого отходить от банкомата.

10. Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.

11. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах.

12. Если при проведении операций с банковской картой в банкомате банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту), которая не была возвращена банкоматом, и далее следовать инструкциям сотрудника кредитной организации.

Рекомендации при использовании банковской карты для безналичной оплаты товаров и услуг.

1. Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.

2. Требуйте проведения операций с банковской картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на банковской карте.

3. При использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской карты предоставить паспорт, подписать чек или ввести ПИН. Перед набором ПИН следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем как подписать чек, в обязательном порядке проверьте сумму, указанную на чеке.

4. В случае если при попытке оплаты банковской картой имела место "неуспешная" операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

Рекомендации при совершении операций с банковской картой через сеть Интернет.

1. Не используйте ПИН при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.

2. Не сообщайте персональные данные или информацию о банковской(ом) карте (счете) через сеть Интернет, например ПИН, пароли доступа к ресурсам банка, срок действия банковской карты, кредитные лимиты, историю операций, персональные данные.

3. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета рекомендуется для оплаты покупок в сети Интернет использовать отдельную банковскую карту (так называемую виртуальную карту) с предельным лимитом, предназначенную только для указанной цели и не позволяющую проводить с ее использованием операции в организациях торговли и услуг.

4. Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг.

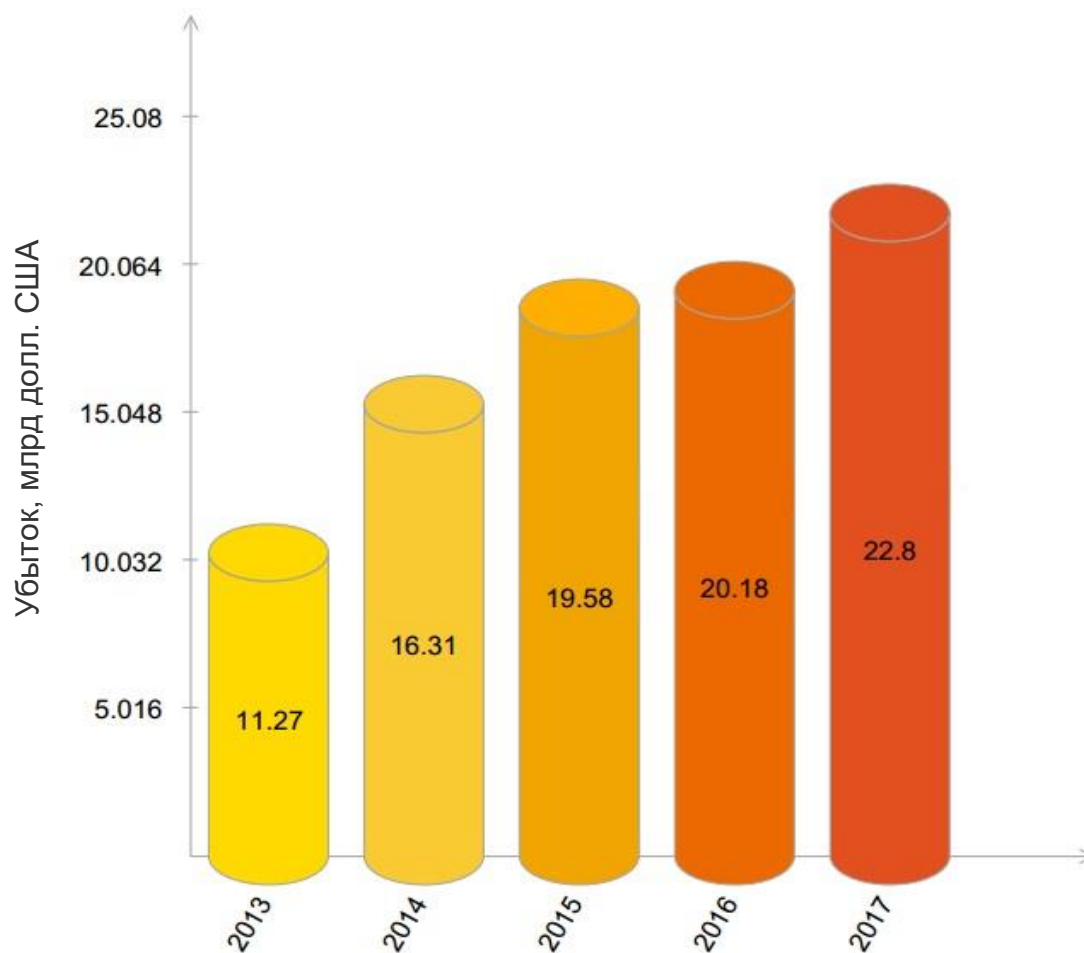
5. Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.

6. Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и (или) информации о банковской(ом) карте (счете). В случае если покупка совершается с использованием чужого компьютера, не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки).

7. Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ), это может защитить Вас от проникновения вредоносного программного обеспечения.

Приложение 5

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 6

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)