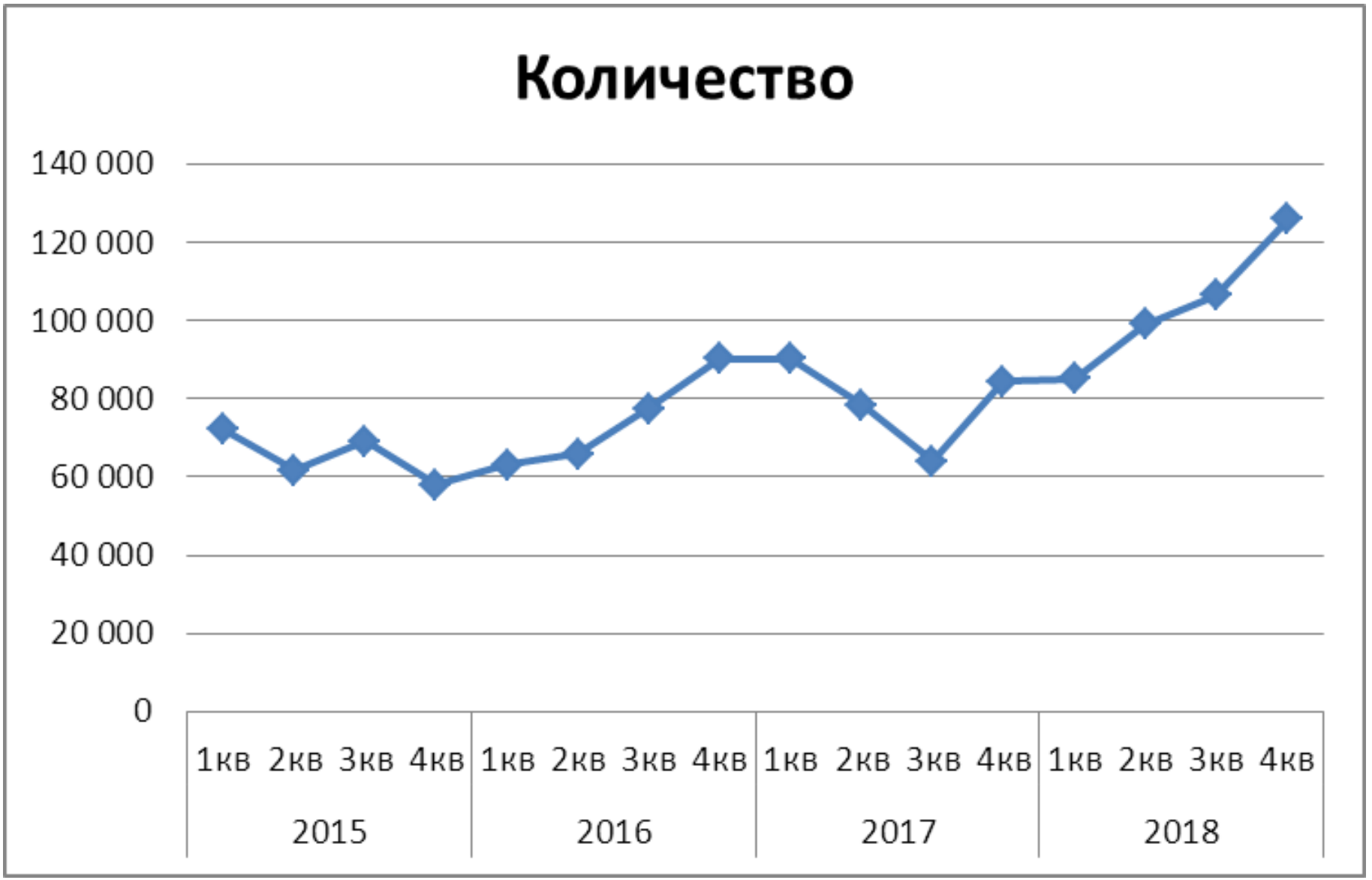
Тенденции в области мошенничества с банковскими картами

Пятиизбянцев Николай Петрович

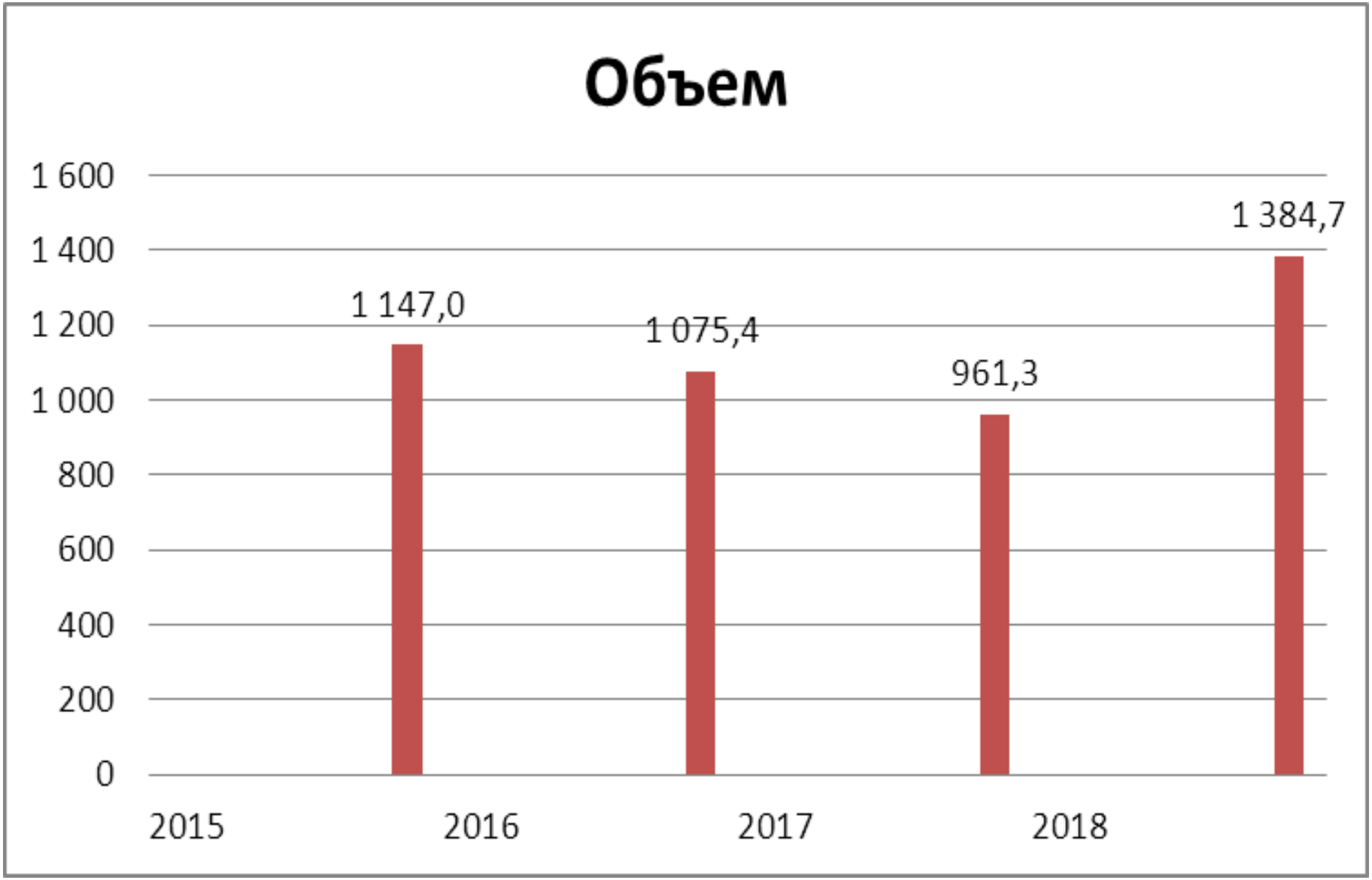
В докладе отражено личное мнение автора, которое не имеет отношения к точке зрения работодателя

ЦБ РФ несанкционированные операции по картам

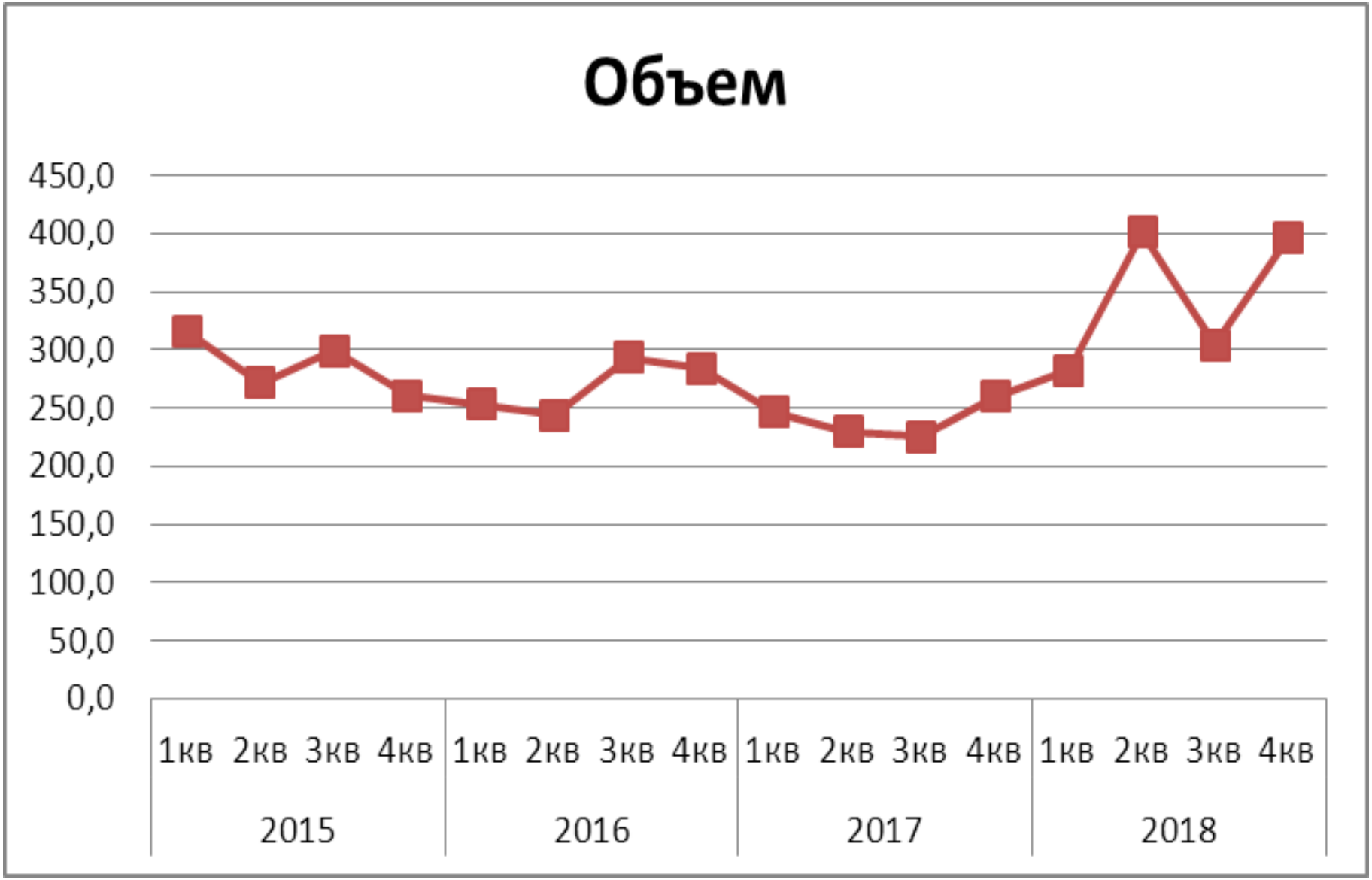
ЦБ РФ несанкционированные операции по картам



ЦБ РФ несанкционированные операции по картам

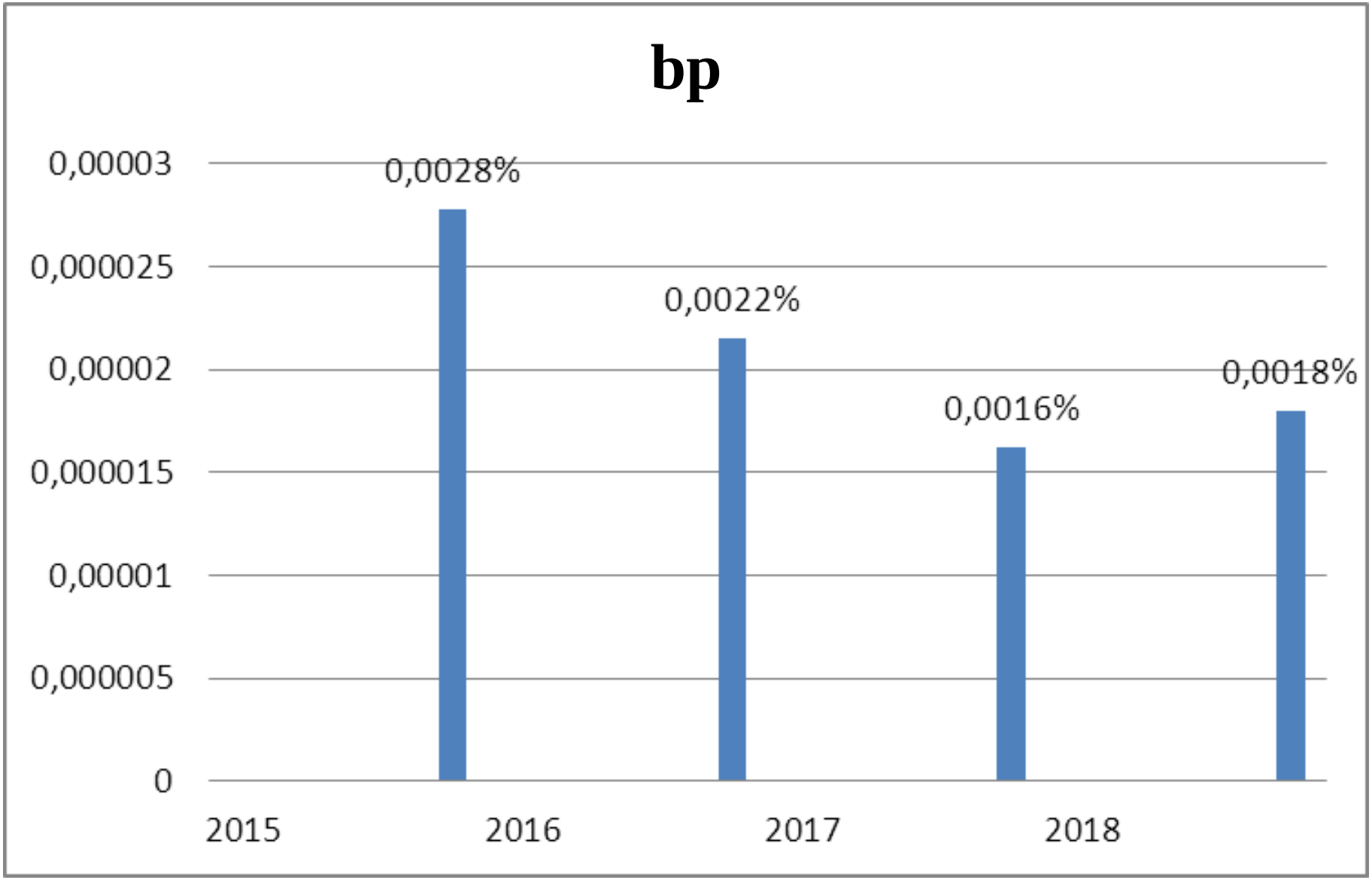


ЦБ РФ несанкционированные операции по картам

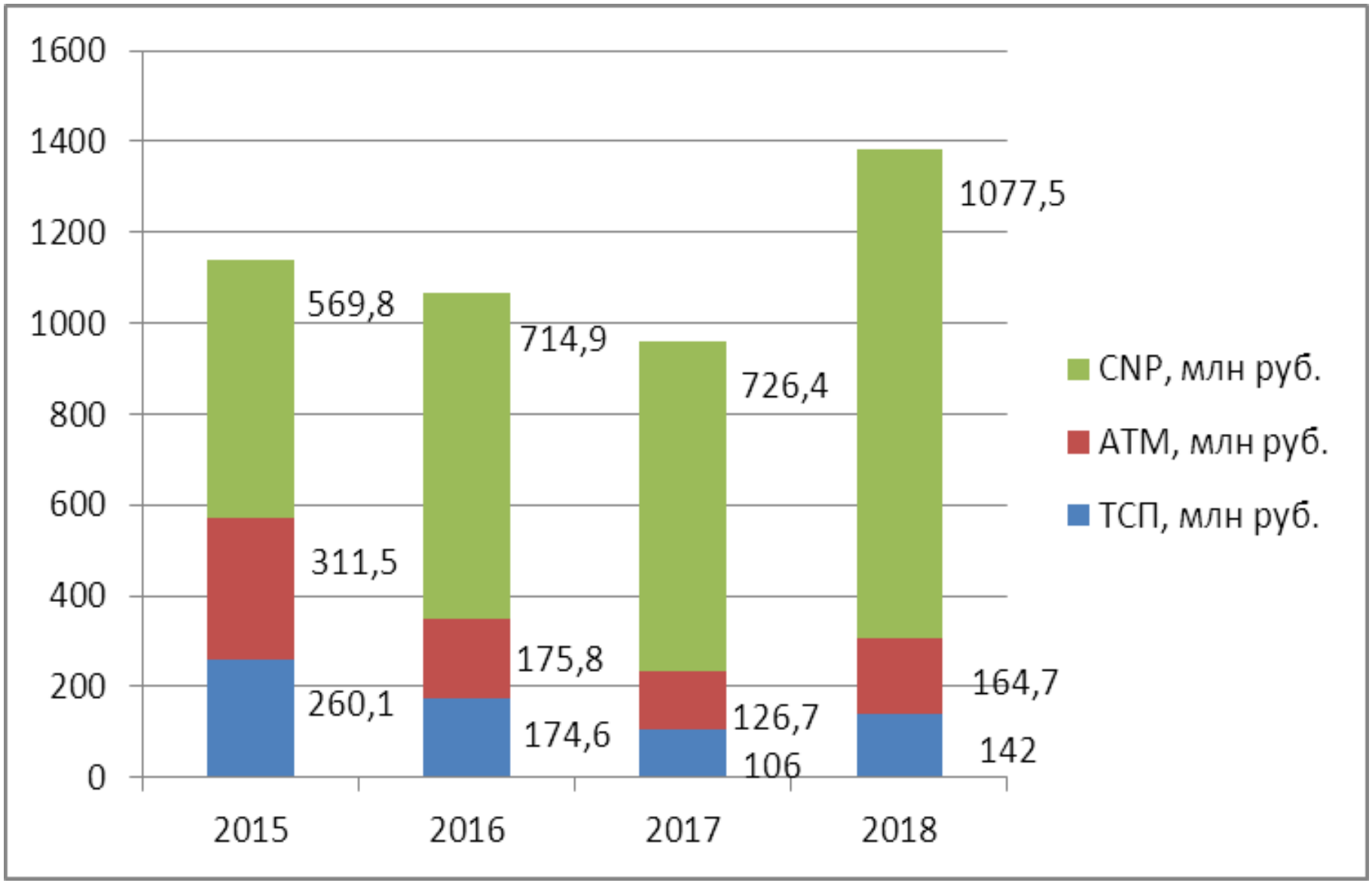


ЦБ РФ несанкционированные операции по картам

ЦБ РФ несанкционированные операции по картам

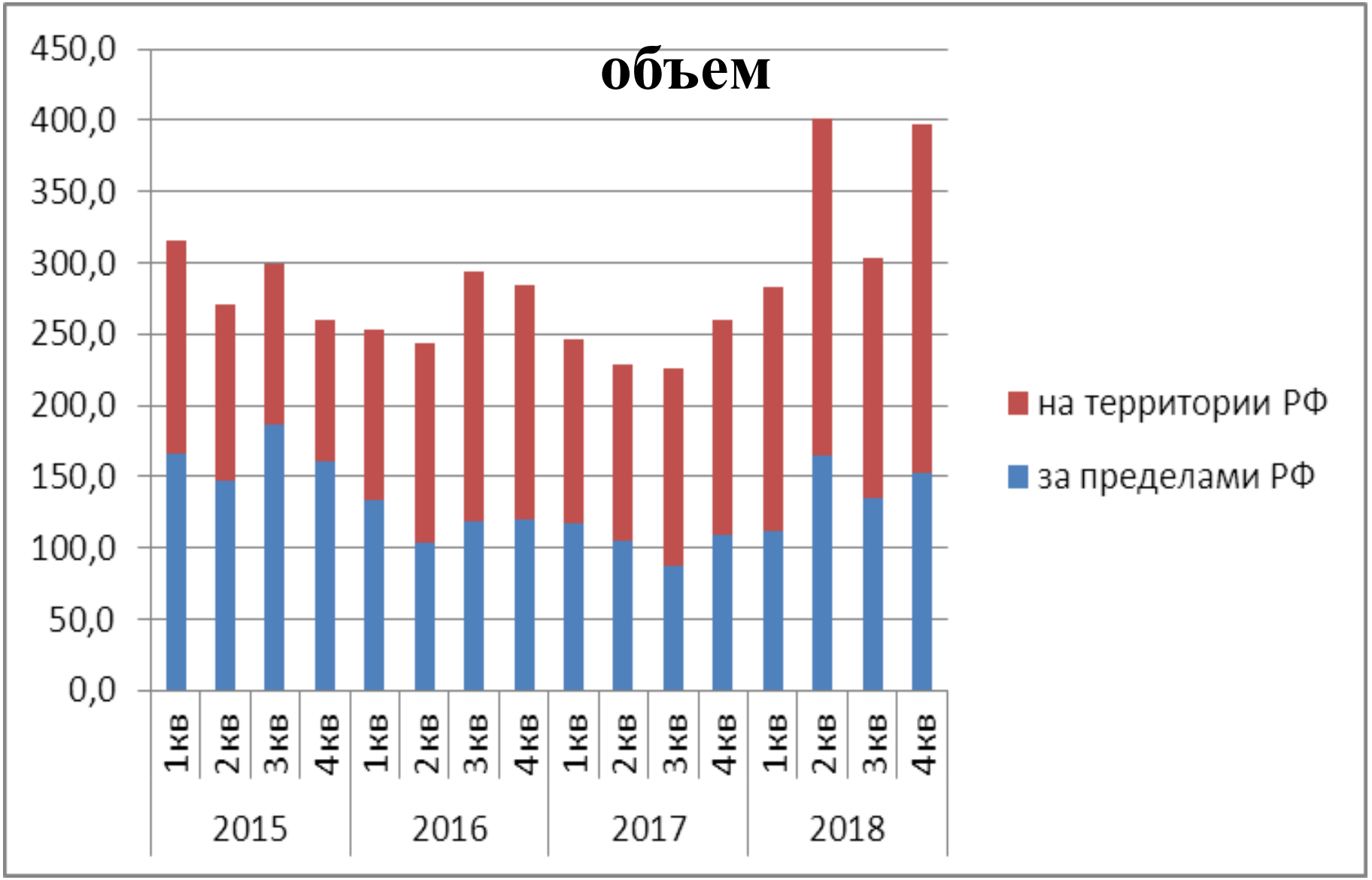


ЦБ РФ несанкционированные операции по картам



ЦБ РФ несанкционированные операции по картам

ЦБ РФ несанкционированные операции по картам



Постановление Пленума ВС РФ

от 30 ноября 2017 г. № 48

Квалификация преступления зависит не только от способа хищения (тайное, путем обмана, открытое, с применением насилия и др.), но и от **способа подготовки** к хищению.

Например:

денежные средства были похищены путем ввода реквизитов карты в сети Интернет и перевода денежных средств с карты держателя на карту мошенника.

Если:

- реквизиты карты были переданы злоумышленнику самим держателем (социальная инженерия), то это кража (158 УК РФ).

- держатель карты ввел реквизиты на фишинговом интернет ресурсе, то это мошенничество (159 УК РФ).

- злоумышленник приобрел реквизиты карты у лица, которое их ранее похитило, то это кража (158 УК РФ).

- держатель сам осуществлял перевод с карты на карту, но вредоносное ПО подменило номер карты получателя, то это компьютерное мошенничество (159.6 УК РФ).

111-ФЗ от 23.04.2018

изменения в Уголовный Кодекс РФ

Часть 3 ст. 158 УК РФ (Кража) была дополнена квалифицирующим признаком:

г) с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 настоящего Кодекса).

Максимальное наказание предусматривает лишение свободы до 6 лет. Преступление — тяжкое, то есть уголовная ответственность наступает, в том числе, за приготовление к преступлению.

111-ФЗ от 23.04.2018

изменения в Уголовный Кодекс РФ

Изменен размер похищенной суммы для статей 159.3 и 159.6 УК РФ, влияющий на квалификацию (крупный, особо крупный).

Снижен с 1,5 миллионов до 250 тысяч и с 6 миллионов до 1 миллиона рублей соответственно.

111-ФЗ от 23.04.2018

изменения в Уголовный Кодекс РФ

Изменилась статья 159.3 (Мошенничество с использованием платежных карт), в новой редакции:

Мошенничество с использованием электронных средств платежа

Предмет преступления **электронные средства платежа** шире, чем платежные карты, определение дано в Федеральном Законе 161-ФЗ «О национальной платежной системе» (п.19 ст.3)

111-ФЗ от 23.04.2018

изменения в Уголовный Кодекс РФ

В новой редакции по ч.1 ст. 159.3 УК РФ максимальное наказание - лишение свободы до 3 лет (ранее арест до 4 месяцев).

Исключен способ хищения «путем обмана уполномоченного работника кредитной, торговой или иной организации».

111-ФЗ от 23.04.2018

изменения в Уголовный Кодекс РФ

Часть 3 ст. 159.6 (Мошенничество в сфере компьютерной информации) дополнена квалифицирующим признаком

в) с банковского счета, а равно в отношении электронных денежных средств

Максимальное наказание по ч.1. данной статьи осталось без изменения — арест до 4 месяцев.

УК РФ

Сравним:

п. г) ч. 3 ст. 158 УК РФ:

Кража (тайное **хищение) совершенная с банковского счета, а равно в отношении электронных денежных средств** (при отсутствии признаков преступления, предусмотренного статьей 159.3 настоящего Кодекса).

Статья 159.3. Мошенничество (**хищение**) с использованием электронных средств платежа

Часть 3 ст. 159.6 УК РФ:

Мошенничество в сфере компьютерной информации, то есть **хищение, совершенное с банковского счета, а равно в отношении электронных денежных средств**.

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Печать

В Красноярском крае полицейские раскрыли кражу с карты, совершенную лжеработником банка

24 Августа 10:50

В дежурную часть ОМВД России по г. Норильску обратилась с заявлением 34-летняя норильчанка, которая рассказала, что с ее банковской карты было списано более 76 тысяч рублей. Полицейские установили, что на телефон потерпевшей позвонил мужчина и представился сотрудником финансового учреждения. В ходе разговора женщина предоставила злоумышленнику все данные карты, после чего с ее счета были списаны денежные средства.

В ходе оперативно-розыскных мероприятий полицейские установили личность 26-летнего подозреваемого, который осуществил звонок из другого региона.

Возбуждено уголовное дело по признакам преступления, предусмотренного частью 3 статьи 158 Уголовного кодекса Российской Федерации «Кража с банковской карты». Санкция данной статьи предусматривает максимальное наказание до шести лет лишения свободы.

Адрес данной страницы в интернете: https://xn--b1aew.xn--p1ai/news/item/14220967

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Печать

В Красноярском крае полицейские раскрыли кражу с карты, совершенную лжеработником банка

24 Августа 10:50

В дежурную часть ОМВД России по г. Норильску обратилась с заявлением 34-летняя норильчанка, которая рассказала, что с ее банковской карты было списано более 76 тысяч рублей. Полицейские установили, что на телефон потерпевшей позвонил мужчина и представился сотрудником финансового учреждения. В ходе разговора женщина предоставила злоумышленнику все данные карты, после чего с ее счета были списаны денежные средства.

Возбуждено уголовное дело по признакам преступления предусмотренного частью 3 статьи 158 Уголовного кодекса Российской Федерации «Кража с банковской карты».

Адрес данной страницы в интернете: https://xn--b1aew.xn--p1ai/news/item/14220967

Статья 274.1 УК РФ

Было	Новое
ст. 274	ч.3 ст.274.1
Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, **причинившее крупный ущерб**	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к КИИ, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно **повлекло причинение вреда КИИ**
до 2 лет	до 6 лет

Часть 3 статьи 274.1 УК РФ

N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Субъекты КИИ - российские юридические лица, которым принадлежат информационные системы, функционирующие в банковской сфере являются субъектами КИИ

Любой сотрудник банка, который нарушил внутренние инструкции, регламенты, положения и т.п. по эксплуатации, обработке, передаче, доступе к охраняемой компьютерной информации, если это причинило (могло причинить) вред (любой) КИИ, может быть привлечен к уголовной ответственности.

Часть 3 статьи 274.1 УК РФ

Уголовная ответственность значительно усилена, предусмотрена за нарушения повлекшие не ущерб в сумме более 1 миллиона рублей, а за причинение вреда.

Вред может быть имущественным (прямые убытки – сломался компьютер, упущенная выгода – программа не работала), деловой репутации (негативные отзывы в соц.сетях).

Нижняя граница вреда не определена.

Часть 3 статьи 274.1 УК РФ

Максимальное наказание - до 6 лет лишения свободы.

По ст. 15 УК РФ преступление является тяжким.

В соответствии со статьями 30 и 66 УК РФ даже за приготовление к тяжкому преступлению предусмотрена уголовная ответственность (наказания не может превышать половины максимального срока).

То есть для привлечения к уголовной ответственности по ч.3 ст. 274.1 УК РФ вред может быть даже не причинен, так как преступление не было окончено, но уголовная ответственность может наступить за приготовление к преступлению или покушение на преступление, если нарушение правил совершено умышленно.

167-ФЗ Стенограммы заседаний ГД РФ

Заседание № 119

О проекте федерального закона № 296412-7 "О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств".

ДИВИНСКИЙ И. Б., фракция "ЕДИНАЯ РОССИЯ".

Уважаемый Александр Дмитриевич, уважаемые коллеги! **Законопроект внесён Правительством Российской Федерации и направлен на предотвращение хищений с банковских счетов организаций, граждан посредством использования банковских карт** через Интернет и мобильные устройства. Законопроект подготовлен к принятию в третьем чтении, прошёл все необходимые экспертизы и согласования.

Прошу проголосовать за принятие законопроекта в третьем чтении.

ПРЕДСЕДАТЕЛЬСТВУЮЩИЙ. Есть ли желающие выступить по мотивам? Нет.

Ставится на голосование в третьем чтении.

Проголосовало за 370 чел. Голосовало 370 чел.

Принят в третьем чтении.

Федеральный закон от 27.06.2018 N 167-ФЗ

При выявлении подозрительной операции банк обязан:

- приостановить: 1) исполнение распоряжения
  2) использование электронного средства платежа
- запросить у клиента подтверждение

При подтверждении

- возобновить: 1) исполнение распоряжения
  2) использование электронного средства платежа

При невозможности связаться

- возобновить через 2 дня: 1) исполнение распоряжения
  2) использование электронного средства платежа

Письмо ЦБ РФ от 7 декабря 2018 г. N 56-3-2/226

Согласно позиции ряда операторов платежных систем с учетом технологии проведения операций по переводу денежных средств с использованием платежных карт под термином "**Приостановление исполнения распоряжения" следует понимать отказ в авторизации** операции, в то время как "**Возобновление исполнения распоряжения" означает обеспечение возможности** проведения по запросу клиента авторизации операции, аналогичной приостановленной по сумме, валюте, получателю и назначению, при наличии доступного остатка денежных средств на банковском счете клиента, к которому привязана платежная карта клиента, либо достаточного кредитного лимита, предоставляемого кредитной организацией - эмитентом клиенту по банковскому счету, к которому привязана платежная карта, либо при наличии у клиента доступного остатка электронных денежных средств, осуществление операций с которыми предусматривает использование платежной карты клиента.

Федеральный закон от 27.06.2018 N 167-ФЗ

Приостановить распоряжение – отказ в авторизации

Возобновить распоряжение - обеспечить возможность проведения авторизации, аналогичной приостановленной

Но банк обязан возобновить:

1) исполнение распоряжения

2) использование электронного средства платежа

Дать возможность провести операцию – это возобновить использование ЭСП

Распоряжение клиент будет давать повторно

Федеральный закон от 27.06.2018 N 167-ФЗ

Признаки осуществления перевода денежных средств без согласия клиента **устанавливаются Банком России:**

3. **Несоответствие** характера, и (или) параметров, и (или) объема проводимой **операции** (время (дни) осуществления операции, место осуществления операции, устройство, с использованием которого осуществляется операция и параметры его использования, сумма осуществления операции, периодичность (частота) осуществления операций, получатель средств) операциям, **обычно совершаемым клиентом** оператора по переводу денежных средств (осуществляемой клиентом деятельности).

Жалоба клиента в ЦБ РФ

Банк России
107016.Москва. улица Неглинная. дом 12

Так, руководствуясь законом от 27.06.2018 № 167-ФЗ, кредитные организации должны внимательнее отслеживать подозрительные транзакции и приостанавливать их. Одним из механизмов является блокировка средства платежа в том случае, если у банка возникает подозрение, что контроль над ним захватил мошенник. Банк обязан незамедлительно связаться с клиентом, если посчитает его транзакцию подозрительной, чтобы подтвердить легитимность этой операции.

Федеральный закон от 27.06.2018 N 167-ФЗ

Необходимо реализовать системы онлайн мониторинга:

Останавливается первая операция - система фрод мониторинга работает «в разрыв»

Серьезная доработка, большие вычислительные мощности, фрод мониторинг становится «бутылочным горлом», увеличивает время транзакции, может привести к отказу «эмитент не доступен»

Любая несанкционированная (мошенническая) операция обычно не совершается клиентом

167-ФЗ > GDPR

Признаки осуществления перевода денежных средств без согласия клиента**:**

3. Несоответствие … **место осуществления операции**

АНТИФРОД

получение информации об операциях клиентов российского банка, находящихся на территории ЕС: международные платежные карты, мобильное приложение, интернет-банк

- мониторинг активности лиц в ЕС, геолокация

– **критерий применимости требований General Data Protection Regulation** (GDPR - «Общего регламента Европейского союза по защите данных»).

GDPR

Подробная информация об условиях и принципах обработки персональных данных в соответствии с GDPR

ПАО Сбербанк

3. Откуда мы собираем персональные данные и с какой целью их обрабатываем

Путем сбора и накопления новых персональных данных в ходе взаимодействия с субъектом (**история** продуктов, **транзакций**, обращений), в ходе использования субъектами персональных данных сайтов и мобильных приложений Банка (**данные о местоположении**, IP-адресах, действиях на сайтах и в приложениях)

https://www.sberbank.ru/ru/personal_policy/gdpr

УКАЗАНИЕ ЦБ РФ от 8.10.2018 г. N 4926-У

Дропы - лица на счета, карты которых перечисляют похищенные денежные средства

2.2. Оператор по переводу денежных средств при реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента **должен**:

реализовывать в отношении клиента - получателя средств, в адрес которого ранее совершались операции по переводу денежных средств без согласия клиента, в случаях, предусмотренных договором банковского счета, **ограничения** по параметрам операций по осуществлению переводов денежных средств (переводов электронных денежных средств) с использованием платежных карт, а также **ограничения** на получение наличных денежных средств в банкоматах за одну операцию и (или) за определенный период времени;

Положение ЦБ РФ № 375-П (115-ФЗ)

п.6.1. Кредитная организация также вправе использовать иные признаки, указывающие на необычный характер сделки, установленные кредитной организацией самостоятельно с целью снижения риска вовлечения кредитной организации в осуществление легализации (отмывания) доходов, полученных преступных путем, и финансирование терроризма.

Дополнительный признак:

Получение в соответствии с п.11.1. ст.9 и п.7 ст.27

161-ФЗ "О национальной платежной системе"

уведомления о приостановлении зачисления денежных средств

или информации о переводе денежных средств без согласия клиента.

Обзор судебной практики

по делам, связанным с защитой прав потребителей финансовых услуг

Утвержден Президиумом ВС РФ 27.09.2017 г.

11. Выдача (замена) сим-карты является услугой связи. **Оператор мобильной связи несет ответственность за неправомерные действия по выдаче дубликата сим-карты** с абонентским номером пользователя другому лицу, последствием которых является получение таким лицом доступа к банковским счетам гражданина, использующего этот абонентский номер с подключением к нему услуги «мобильный банк».

Определение судебной коллегии по гражданским делам ВС РФ от 24.04.2018 №5-КГ18-41

Определение судебной коллегии

по гражданским делам ВС РФ от 10.01.2017 г. № 4-КГ16-66

Договором может быть предусмотрено удостоверение прав распоряжения денежными суммами, находящимися на счете, электронными средствами платежа и другими документами с использованием в них аналогов собственноручной подписи, кодов, паролей …

По смыслу приведенных правовых норм, банк несет риск ответственности за последствия исполнения поручений, выданных неуполномоченными лицами.

для подтверждения распоряжения о переводе денежных средств на соответствующий абонентский номер Банком направлялись неперсонифицированные пароли, требующие введения определенной комбинации символов для подтверждения ранее направленного распоряжения.

Определение судебной коллегии

по гражданским делам ВС РФ от 10.01.2017 г. № 4-КГ16-66

Такие меры направлены, главным образом, на предотвращение исполнения ошибочных и случайных распоряжений, однако **из этого не следует, что таким образом идентифицируется владелец счета** либо его доверенное лицо, владеющее соответствующим кодом или паролем.

Напротив, операция по введению направленного банком одноразового неперсонифицированного **пароля доступна любому лицу, использующему в данный момент абонентское устройство подвижной телефонной сети**.

Апелляционное определение судебной коллегии по гражданским делам Московского областного суда от 4 апреля 2016 г. отменить

сбп

система быстрых платежей

I этап: переводы между физическими лицами

«Известия» провели эксперимент и перечислили через СБП

10 рублей главе Казначейства России Роману Артюхину.

При этом **на экране телефона** даже **высветился полный номер его счета**.

После того как с карты корреспондента издания списались деньги, **пришло СМС**, что перевод выполнен, а его **получатель — «Артюхин Роман Евгеньевич»**.

https://www.banki.ru/news/lenta/?id=10886012

Информационный поток между мобильным приложением и банком является проприетарным (то есть не регулируемым Стандартом НСПК)

I этап: переводы между физическими лицами

Банки Участники СБП получают информацию о клиентах (ФИО, номер телефона, банк) других Участников

Данную информацию можно проанализировать с целью предложения клиентам других Участников заведомо более выгодных условий обслуживания (не соответствует целям обработки персональных данных в рамках СБП)

С учетом ЕБС можно привлекать таких клиентов удаленно

Следствие – отток клиентов

I этап: переводы между физическими лицами

Статья 204 УК РФ. Коммерческий подкуп

5. Незаконное получение лицом, выполняющим управленческие функции в коммерческой или иной организации, денег

- наказывается лишением свободы на срок:

до 3 лет

в значительном размере (> 25 т.р.) - до 5 лет

в крупном размере (> 150 т.р.) – от 5 до 9 лет

в особо крупном размере (> 1 млн р.) - от 7 до 12 лет

СБП – переводы до 600 т.р.

I этап: переводы между физическими лицами

Статья 290 УК РФ. Получение взятки

1. Получение должностным лицом, иностранным должностным лицом либо должностным лицом публичной международной организации лично или через посредника взятки в виде денег,

- наказывается лишением свободы на срок:

до 3 лет

в значительном размере (> 25 т.р.) - до 6 лет

в крупном размере (> 150 т.р.) – от 7 до 12лет

в особо крупном размере (> 1 млн р.) - от 8 до 15 лет

СБП – переводы до 600 т.р.

I этап: переводы между физическими лицами

Постановление Пленума Верховного Суда РФ от 9 июля 2013 г. N 24 "О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях"

10. **Получение** и дача взятки, а равно незаконного вознаграждения при коммерческом подкупе, посредничество во взяточничестве в виде непосредственной передачи взятки **считаются оконченными с момента** принятия должностным лицом либо лицом, выполняющим управленческие функции в коммерческой или иной организации, хотя бы части передаваемых ему ценностей (например, с момента передачи их лично должностному лицу, **зачисления с согласия должностного лица на счет, владельцем которого оно является**). При этом **не имеет значения**, получили ли указанные лица реальную возможность пользоваться или распоряжаться переданными им ценностями по своему усмотрению.

I этап: переводы между физическими лицами

Постановление Пленума Верховного Суда РФ от 9 июля 2013 г. N 24 "О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях"

24. **Получение** должностным лицом либо лицом, выполняющим управленческие функции в коммерческой или иной организации, **ценностей** за совершение действий (бездействие), которые входят в его полномочия либо которые оно могло совершить с использованием служебного положения, **следует квалифицировать как получение взятки** либо коммерческий подкуп **вне зависимости от намерения совершить указанные действия** (бездействие)

I этап: переводы между физическими лицами

Статья 304 УК РФ. Провокация взятки, коммерческого подкупа либо подкупа в сфере закупок товаров, работ, услуг для обеспечения государственных или муниципальных нужд

Провокация взятки, коммерческого подкупа либо подкупа в сфере закупок …

попытка передачи …

без его согласия денег …

в целях искусственного создания доказательств совершения преступления или шантажа, -

наказывается лишением свободы на срок до пяти лет

Федеральный закон от 27.06.2018 N 167-ФЗ

При выявлении подозрительной операции банк обязан:

- приостановить исполнение распоряжения

- запросить у клиента подтверждение

При подтверждении возобновить исполнение распоряжения

Для СБП:

Банк плательщика передает клиенту (плательщику) данные получателя (РАМ) и запрашивает подтверждение перевода

Плательщик проверяет РАМ и подтверждает перевод

167-ФЗ выполнен!

II этап: платежи физических лиц в адрес юридических лиц за товары и услуги

Если тарифы СБП будут меньше эквайринговых комиссий

Конкуренция карточным платежным системам

Следствие: нет договора эквайринга
не действует PCI DSS (нет номеров карт)

II этап: платежи физических лиц в адрес юридических лиц за товары и услуги

Нет договора эквайринга -

нет требований МПС и МИР к ТСП со стороны эквайрера:

- проверка ТСП на моменте привлечения (экономическое обоснование, проверка экономической безопасности, инспекция ТСП, список недобросовестных ТСП от ПС)

- дальнейшая работа по управлению рисками, фрод-мониторинг, защита бренда (запрещенный товар, в т.ч. контрафакт)

Нет ответственности эквайрера за неоказанную со стороны ТСП услугу (мошенники, Трансаэро, Натали турс)

Программы МПС: агрегаторы, высокорискованные ТСП

II этап: платежи физических лиц в адрес юридических лиц за товары и услуги

Физические лица плательщики окажутся со своими проблемами наедине с недобросовестными ТСП и мошенниками

Рынок ТСП может превратиться из цивилизованного (карточного) в дикий

Нужны Правила, Программы аналогичные МПС

Участники СБП – банки клиенты ЦБ РФ и участники ПС МИР

Если ТПС заинтересован в клиентах иностранных банков, будет принимать карты МПС

Если иностранцы платят по карте, а россияне СБП, права россиян защищены меньше

СБП - карты

Если

СБП – зарплатные проекты, бюджетные выплаты

СБП – получение наличных АТМ

СБП – переводы заграницу

Положение ЦБ 382-П – российская криптография МИР

СБП – прямой конкурент карте МИР

Если физ.лицо заинтересовано платить в зарубежных ТСП, в т.ч. онлайн – карты МПС

СПАСИБО!