ОБЗОР ОПЕРАЦИЙ, СОВЕРШЕННЫХ БЕЗ СОГЛАСИЯ КЛИЕНТОВ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ ЗА 2019 ГОД

Банк России

СОДЕРЖАНИЕ

Материал подготовлен Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Департамента информационной безопасности Банка России.

Фото на обложке: Shutterstock/FOTODOM

107016, Москва, ул. Неглинная, 12
Официальный сайт Банка России: www.cbr.ru

СПИСОК СОКРАЩЕНИЙ

АСОИ ФинЦЕРТ	Автоматизированная система обработки инцидентов
АС «Фид-АнтиФрод»	Автоматизированная система «Фид-АнтиФрод»
ВПО	Вредоносное программное обеспечение
ДБО	Дистанционное банковское обслуживание
Комплекс БР ИББС	Комплекс документов Банка России по стандартизации обеспечения информационной безопасности организаций банковской системы Российской Федерации, описывающий единый подход к построению системы обеспечения информационной безопасности организаций банковской сферы с учетом требований российского законодательства
Мобильные устройства	Абонентские устройства мобильной связи, мобильные телефоны, смартфоны, коммуникаторы и другие устройства, используемые клиентами кредитных организаций при осуществлении переводов денежных средств
Операции без согласия клиентов	Операции по переводу денежных средств, соответствующие утвержденным приказом Банка России от 27 сентября 2018 г. № ОД-2525 признакам осуществления перевода денежных средств без согласия клиента
Положение Банка России № 382-П	Положение Банка России от 9.06.2012 № 382-П «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»
Федеральный закон № 161-ФЗ	Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе»
Федеральный закон № 167-ФЗ	Федеральный закон от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств»
Форма отчетности 0403203	Форма отчетности 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств», установленная Указанием Банка России от 9.06.2012 № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств»
Форма отчетности 0409258	Форма отчетности 0409258 «Сведения о несанкционированных операциях, совершенных с использованием платежных карт», установленная Указанием Банка России от 24 ноября 2016 г. № 4212-У «О перечне, формах и порядке составления и представления форм отчетности кредитных организаций в Центральный банк Российской Федерации»
ЭСП	Электронное средство платежа
CNP-транзакция	Транзакция типа «Card Not Present» – операция, осуществленная в сети Интернет с использованием реквизитов платежной карты (без предъявления ее материального носителя)

ВВЕДЕНИЕ

Анализ и мониторинг операций, совершаемых без согласия клиентов кредитных и некредитных финансовых организаций в кредитно-финансовой сфере, является задачей ФинЦЕРТ уже более четырех лет. Цель этой деятельности – их выявление и предотвращение совместно с участниками информационного обмена, а также формирование базы знаний о структуре указанных операций.

В настоящем обзоре приведены данные о количестве и объеме операций, совершенных без согласия клиентов за 2019 год. Обзор составлен на основе сведений, предоставленных отчитывающимися операторами по переводу денежных средств и операторами услуг платежной инфраструктуры в Банк России в рамках форм отчетностей 0403203 и 0409258.

В большинстве случаев данные за 2019 г. приводятся по форме 0403203, в то время как в предыдущем обзоре они предоставлялись в соответствии с формой отчетности 0409258. Это сделано для того, чтобы представить более полную и соответствующую реальному положению дел картину, целью чего и было изменение формы 0403203.

Как и предполагалось годом ранее, изменение в 2018 г. формы отчетности 0403203, а также усиление ответственности участников кредитно-финансовой сферы за полное и своевременное предоставление данных обусловили ощутимое улучшение качества предоставляемых данных и их объем.

Настоящий обзор может быть использован операторами по переводу денежных средств, а также операторами услуг платежной инфраструктуры в целях планирования мероприятий по управлению рисками, внутреннему контролю, защите информации, в том числе в целях учета количества и характера инцидентов, произошедших при эксплуатации объектов информационной инфраструктуры, реализации требований к обеспечению защиты информации при осуществлении переводов денежных средств.

ОБЩИЕ СВЕДЕНИЯ ОБ ОПЕРАЦИЯХ БЕЗ СОГЛАСИЯ КЛИЕНТОВ

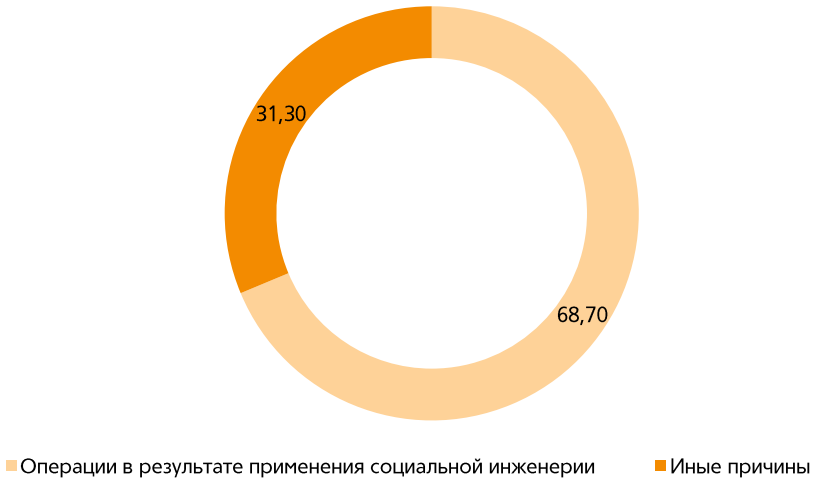
Изменение в 2018 г. формы отчетности 0403203, а также усиление ответственности участников кредитно-финансовой сферы за полное и своевременное предоставление данных обусловили ощутимое повышение качества предоставляемых данных и их объем. Запуск АСОИ ФинЦЕРТ и АС «Фид-Антифрод» позволил повысить выявляемость операций без согласия клиентов. В результате полученные от кредитных организаций данные продемонстрировали рост показателей количества и объема хищений в 2019 году.

В 2019 г. объем всех операций, совершенных без согласия клиентов (физических и юридических лиц) с использованием электронных средств платежа, составил 6426,5 млн рублей. Количество таких операций – 576 566 единиц.

Средняя сумма одной операции без согласия клиента по счетам физических лиц в 2019 г. составила 10 тыс. руб., юридических лиц – 152 тыс. рублей.

69% всех операций без согласия клиентов было совершено в результате побуждения клиентов к самостоятельному проведению операции путем обмана или злоупотребления доверием (методами так называемой социальной инженерии).

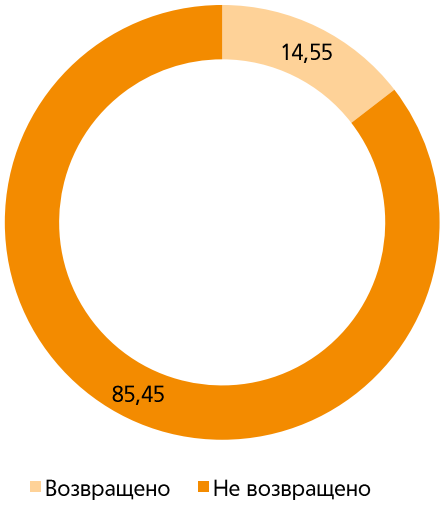
Рисунок 1
Причины совершения операций без согласия клиентов (%)



Банки возместили клиентам 935 млн руб. (15%, или каждый 7-й похищенный рубль). Текущий уровень возмещения объясняется высокой долей социальной инженерии среди операций без согласия клиентов, которые в результате обмана или злоупотребления доверием нарушают условия договора с кредитными организациями, предусматривающие необхо-

димость сохранения конфиденциальности платежной информации. В связи с этим Банк России намерен рассмотреть возможность изменения процедуры возврата (компенсации) похищенных средств клиентов.

Рисунок 2
Возмещение клиентам (%)



СВЕДЕНИЯ ОБ ОПЕРАЦИЯХ БЕЗ СОГЛАСИЯ КЛИЕНТОВ – ФИЗИЧЕСКИХ ЛИЦ[1]

ДИНАМИКА КОЛИЧЕСТВА И ОБЪЕМА ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА (ВКЛЮЧАЯ ПЛАТЕЖНЫЕ КАРТЫ)

По данным Банка России, количество и объем операций по переводу денежных средств с использованием электронных средств платежа (ЭСП) физических лиц составляют 40,3 млрд единиц и 71,03 трлн руб. соответственно. Количество и объем операций с использованием платежных карт (в банкоматах и в Интернете) составили 39,2 млрд единиц и 63,7 трлн руб. соответственно, аналогичные показатели по операциям в системе дистанционного банковского обслуживания (ДБО) – 1,1 млрд единиц и 7,3 трлн руб. соответственно.

С учетом реализации задачи Банка России по повышению доступности финансовых инструментов и развитию новых финансовых технологий, а также влияния естественных факторов конкуренции на развитие кредитно-финансовой сферы мы продолжаем исходить из прогноза роста количества и объема этих операций в планировании работы по повышению информационной безопасности финансовых организаций. При этом Банк России учитывает, что недоверие клиентов, использующих финансовые услуги, к безопасности дистанционных банковских сервисов может отрицательно влиять на эту динамику и сдерживать рост рынка в целом. Таким образом, повышение безопасности финансовых услуг является той задачей, которую Банк России реализует в интересах как их потребителей, так и самих кредитно-финансовых организаций.

КОЛИЧЕСТВО И ОБЪЕМ ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТОВ

Показатели количества и объема операций без согласия клиентов – физических лиц в данном обзоре приводятся в соответствии с данными новой формы отчетности 0403203, используемой с середины 2018 года. Это связано с необходимостью оперировать более полными показателями. Однако для подкрепления и верификации этих данных используется информация из формы 0409258.

Объем всех операций, совершенных без согласия клиентов с использованием ЭСП, в 2019 г. составил 5723,5 млн рублей. Количество таких операций – 571 957 единиц.

Операции, совершенные без согласия клиентов с использованием ЭСП, можно разделить на три типа:

- операции через банкоматы, терминалы и импринтеры;

[1] *Годом ранее ФинЦЕРТ оперировал показателем «несанкционированная операция», который сейчас сохранился в форме отчетности 0409258.*

- оплата товаров и услуг в Интернете (CNP-транзакции);
- операции в системе ДБО.

Необходимо отметить, что большая часть операций без согласия клиентов – физических лиц совершается в результате получения злоумышленниками несанкционированного прямого доступа к электронным средствам платежа либо побуждения владельцев средств самостоятельно совершить перевод в пользу мошенников путем обмана или злоупотребления доверием (с использованием методов социальной инженерии).

ДОЛЯ ОБЪЕМА ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТОВ В ОБЩЕМ ОБЪЕМЕ ОПЕРАЦИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ПЛАТЕЖНЫХ КАРТ

Доля объема операций без согласия клиентов в общем объеме операций, совершенных с использованием платежных карт, в 2019 г. составила 0,0023% (в 2018 г. – 0,0018%). Указанные значения не превышают установленный Банком России целевой показатель доли таких операций в общем объеме операций, совершенных с использованием платежных карт. Этот показатель установлен на уровне 0,005%.

Наблюдаемое в отчетном периоде изменение нисходящей динамики 2015–2017 гг., а также качественно более высокие показатели операционной отчетности указывают на имевшую место реальную необходимость повышения прозрачности предоставляемых банками данных и подтверждают правильность разработки и внедрения мер по минимизации риска осуществления операций без согласия клиентов, принимаемых участниками рынка и Банком России, а также необходимость их дальнейшего развития.

РАСПРЕДЕЛЕНИЕ ПО УСЛОВИЯМ СОВЕРШЕНИЯ ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТОВ

В соответствии с правилами заполнения форм отчетности, направляемых в Банк России, операции без согласия клиентов – физических лиц разделены на группы, исходя из условий их проведения:

- в системе ДБО;
- через банкоматы, терминалы, импринтеры;
- CNP-транзакции.

Как и годом ранее, основную долю по объему и количеству указанных операций составляют CNP-транзакции.

В 2019 г. было зафиксировано 40 тыс. случаев использования платежных карт (за исключением предоплаченных) без согласия их владельцев в банкомате или терминале. Из них почти четверть (22,4%) произошли в результате использования злоумышленниками приемов социальной инженерии. Общая сумма ущерба по хищениям через банкоматы и терминалы составила свыше 525 млн руб., при этом банки вернули клиентам более 10% похищенных средств (54,4 млн руб.).

Больше всего операций без согласия клиентов – физических лиц пришлось на операции по оплате товаров и услуг в Интернете (CNP-транзакции).

Клиенты банков сообщили в прошедшем году о 371,1 тыс. таких транзакций, 2/3 из которых (243,3 тыс. транзакций) – результат применения к ним методов социальной инженерии. Сумма ущерба составила 2971,3 млн руб., при этом банки возместили клиентам примерно каждый 5-й похищенный рубль (всего 653,2 млн руб.).

После принятия федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Гражданский процессуальный кодекс Российской Федерации» (законопроект № 605945-7) у Банка России появятся полномочия по «внесудебной» блокировке фишинговых сайтов в результате прямого взаимодействия с Роскомнадзором по вопросам включения сайтов в реестр запрещенной к распространению на территории Российской Федерации информации.

Указанный законопроект предполагает также введение судебного механизма блокировки сайтов, распространяющих вредоносное программное обеспечение. Банк России получит право обращаться в суд с заявлением в защиту прав, свобод и законных интересов неопределенного круга лиц в связи с размещением в информационно-телекоммуникационных сетях, в том числе в сети Интернет, указанной информации.

Системы дистанционного банковского обслуживания физических лиц становились мишенью мошенников 160,8 тыс. раз, однако доля социальной инженерии в их общем числе самая высокая – порядка 88,9%. Это объясняется целевым характером атак, который в свою очередь обусловлен потенциально более высоким «доходом» злоумышленника (объем остатка на клиентских счетах, доступных в ДБО, может существенно превышать размер средней сделки в Интернете). Объем хищений составил порядка 2227 млн руб., при этом банки вернули клиентам всего 162,3 млн руб., то есть каждый 14-й рубль.

Противодействие мобильному мошенничеству также требует дополнительной разработки регулятивных документов. При участии Банка России готовятся поправки в Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», предусматривающие создание единого канала обмена между операторами связи и банками данными о мобильных устройствах и абонентах.

РАСПРЕДЕЛЕНИЕ ПО ПРИЧИНАМ СОВЕРШЕНИЯ ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТОВ

Как и годом ранее, в качестве способа подавляющего большинства хищений отчитывающиеся операторы указывают социальную инженерию. По итогам 2019 г. ее доля составила почти 69% случаев (в 2018 г. – 97%).

Данное снижение может объясняться, с одной стороны, изменением методики подсчета базовых показателей, с другой – повышением уровня киберграмотности населения в результате проводимых отчитывающимися операторами (в рамках подпункта 2.12.3 Положения Банка России № 382-П) и Банком России мероприятий по повышению осведомленности клиентов банков о рисках использования электронных средств платежа.

Стоит отметить, что отчитывающиеся операторы при указании причин операций без согласия клиентов – физических лиц основываются на данных, предоставленных клиентом при обращении, что является важным источником информации для формирования понимания типа операции.

Кроме того, операторам следует улучшать качество проводимой работы по доведению до клиентов информации о возможных рисках использования ЭСП и о разграничении ответственности банка и клиента в случае компрометации данных платежных карт. При этом указанную работу операторы должны проводить на постоянной основе в соответствии с законодательством Российской Федерации.

РАСПРЕДЕЛЕНИЕ КОЛИЧЕСТВА И ОБЪЕМА ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТОВ ПО МЕСТУ СОВЕРШЕНИЯ ОПЕРАЦИИ

На рисунке 3 представлена информация по распределению операций без согласия клиентов по месту совершения операций. Учтены только данные об операциях, совершенных в банкоматах (терминалах или импринтерах), а также CNP-транзакции по платежным картам, эмитированным на территории Российской Федерации (за исключением Московского региона, на который приходится 339 522 операции без согласия клиентов на сумму 2594 млн руб.). Особенностью рассмотрения территориального распределения указанных операций является их сосредоточение на территории Центрального федерального округа. Это обусловлено нахождением в ЦФО большинства кредитных организаций, обслуживающих физических лиц.

Кредитным организациям в регионах, указанных в таблице 1, необходимо уделять повышенное внимание исполнению подпункта 2.12.3 Положения Банка России № 382-П, обязывающего кредитные организации проводить мероприятия по повышению осведомленности работников и клиентов в области обеспечения защиты информации и рисков получения несанкционированного доступа к электронным денежным средствам.

Рисунок 3
Количество и объем переводов денежных средств без согласия клиента по месту совершения операции (без учета Московского региона)

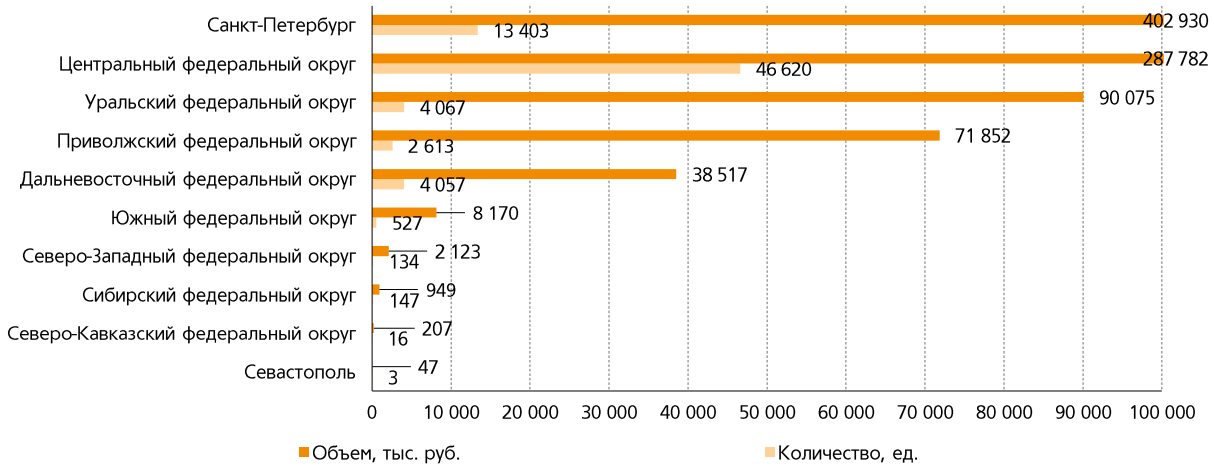


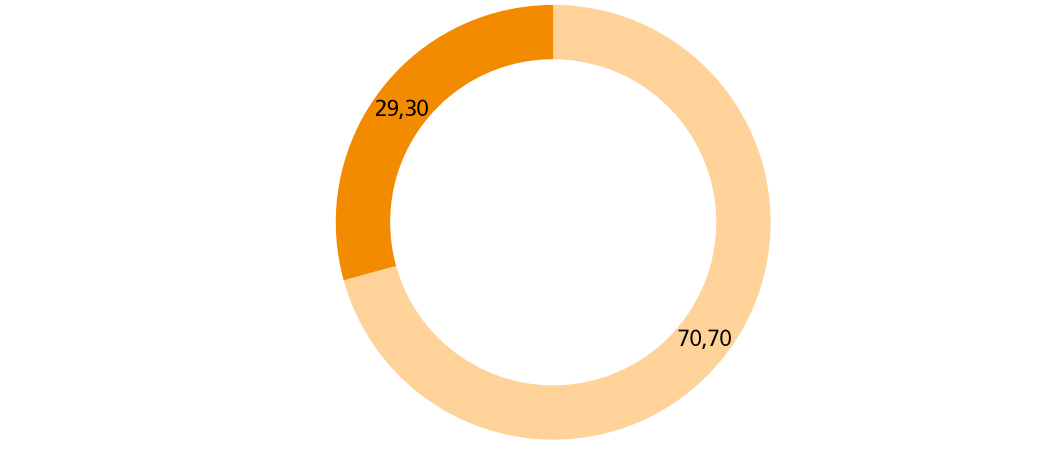
Таблица 1
Количество и объем переводов денежных средств без согласия клиента по месту совершения операции

	Количество, ед.	Объем, тыс. руб.
Москва	339 522	2 593 875
Санкт-Петербург	13 403	402 930,4
Костромская область	46 353	285 878,2
Свердловская область	1 920	70 744,69
Ульяновская область	2	31 575,86
Амурская область	2 627	25 328,57
Республика Татарстан	1 547	19 837,44
Тюменская область	1 605	13 726,22
Приморский край	1 384	10 812,21
Удмуртская Республика	170	7 222,28
Краснодарский край	390	5 794,73
Челябинская область	542	5 603,82
Кировская область	526	5 069,36
Нижегородская область	137	3 920,63
Республика Саха (Якутия)	40	2 298,87
Оренбургская область	86	2 283,89
Ростовская область	115	1 884,27
Пермский край	66	1 438
Вологодская область	89	1 386,97
Курская область	121	599,99
Новосибирская область	85	567,55
Калининградская область	32	537,57
Калужская область	22	521
Республика Крым	21	474,88
Московская область	63	406,75
Самарская область	46	237,65
Республика Мордовия	22	207,87
Ставропольский край	16	207
Новгородская область	12	197,95
Липецкая область	38	158,73
Красноярский край	41	151,79
Томская область	4	125,14
Тульская область	7	95,14
Республика Хакасия	9	85,2
Сахалинская область	6	77,77
Ивановская область	10	73,42
Севастополь	3	47,28
Саратовская область	6	44,55
Рязанская область	4	29,77

	Количество, ед.	Объем, тыс. руб.
Астраханская область	1	15,96
Чувашская Республика	5	14,55
Владимирская область	1	10
Омская область	1	9,59
Ярославская область	1	9
Иркутская область	2	6,95
Кемеровская область	5	2,46
Республика Коми	1	0,07

Рисунок 5
Количество несанкционированных операций с использованием платежных карт в территориальном разрезе (%)

Рисунок 4
Объем операций без согласия клиентов с использованием платежных карт в территориальном разрезе (%)



На операции, совершенные без согласия клиентов за пределами Российской Федерации, приходится 42,5% от количества и 29,3% от объема всех операций без согласия (в 2018 г. аналогичные показатели составили 44 и 40,7% соответственно).

Как и годом ранее, это указывает на необходимость информирования кредитными организациями своих клиентов о возможных рисках при осуществлении трансграничных операций по переводу денежных средств. При этом опубликованные Банком России признаки осуществления переводов денежных средств без согласия клиентов позволят операторам совершенствовать работу антифрод-систем при выявлении трансграничных операций, совершаемых без согласия клиентов.

В связи с этим мы прогнозируем сохранение тенденции, при которой доля объема и количества операций без согласия клиентов, совершенных на территории Российской Федерации, в общем объеме и количестве всех операций без согласия клиентов составляет более 50%.

2. СВЕДЕНИЯ ОБ ОПЕРАЦИЯХ БЕЗ СОГЛАСИЯ КЛИЕНТОВ СО СЧЕТОВ ЮРИДИЧЕСКИХ ЛИЦ

ДИНАМИКА КОЛИЧЕСТВА И ОБЪЕМА ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТОВ

В настоящем обзоре под операциями без согласия клиентов со счетов юридических лиц понимаются события, по которым клиенты сообщили о хищениях средств в результате несанкционированного доступа к системам (средствам) ДБО юридических лиц, индивидуальных предпринимателей и лиц, занимающихся частной практикой, включая системы (средства), используемые для переводов денежных средств по корреспондентским счетам юридических лиц.

В 2019 г. юридические лица сообщили в банки о 4609 операциях без согласия клиента на общую сумму 701 млн рублей.

Порядка 10% похищенных средств (65 млн руб.) компенсированы либо возвращены пострадавшим организациям.

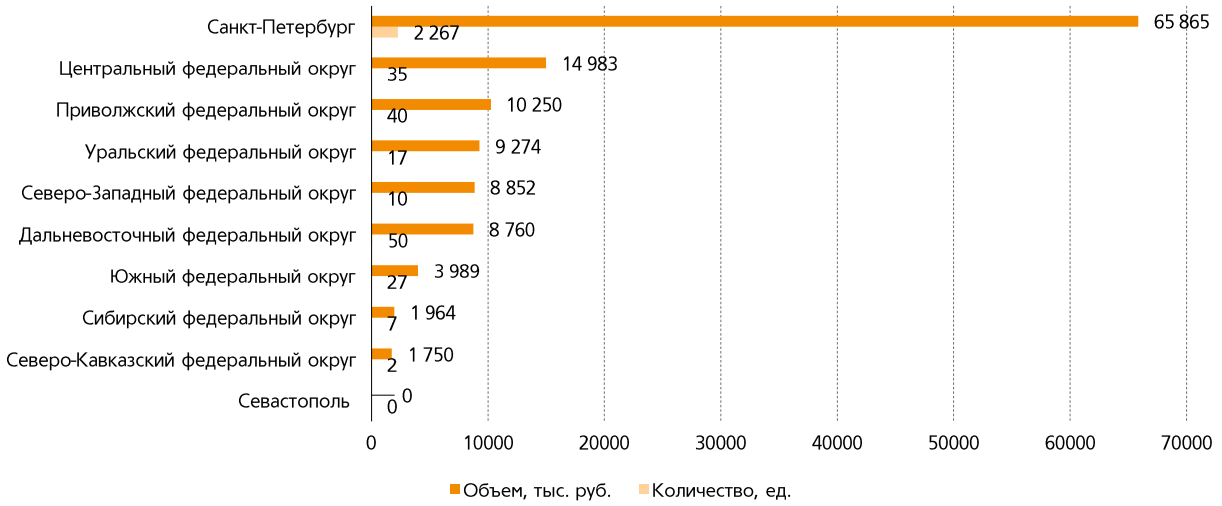
РАСПРЕДЕЛЕНИЕ ПО ПРИЧИНАМ СОВЕРШЕНИЯ ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТОВ

Данные, предоставленные отчитывающимися операторами, свидетельствуют о том, что операции без согласия клиентов – юридических лиц происходили в результате воздействия социальной инженерии в 16% случаев (723 хищения). Сюда относятся в первую очередь инциденты, связанные с получением злоумышленниками доступа к системе ДБО с использованием ВПО, рассчитанного на взлом программного обеспечения стационарных компьютеров. Полагаем, что проблема останется актуальной и в 2020 году. В качестве рекомендаций следует указать необходимость повышения качества работы отчитывающихся операторов в области осведомления своих клиентов в вопросах киберграмотности.

РАСПРЕДЕЛЕНИЕ КОЛИЧЕСТВА И ОБЪЕМА ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТОВ ПО МЕСТУ СОВЕРШЕНИЯ ОПЕРАЦИЙ

В приведенных данных по распределению операций без согласия клиентов со счетов юридических лиц по месту совершения операций указываются данные по месту обращения юридического лица при ее выявлении, то есть по месту ведения счета. Большинство операций без согласия клиентов со счетов юридических лиц посредством использования системы ДБО, как и в 2018 г., совершается на территории Центрального федерального округа. Указанная тенденция обусловлена высокой концентрацией юридических лиц на территории ЦФО, которые привлекают злоумышленников.

Рисунок 6
Количество и объем переводов денежных средств без согласия клиента по месту совершения операции (без учета Московского региона)



Кредитным организациям в регионах, указанных в таблице 2, необходимо уделять повышенное внимание исполнению подпункта 2.12.3 Положения Банка России № 382-П, обязывающего кредитные организации проводить мероприятия по повышению осведомленности работников и клиентов в области обеспечения защиты информации и рисков получения несанкционированного доступа к электронным денежным средствам.

Таблица 2
Количество и объем переводов денежных средств без согласия клиента по месту совершения операции

	Количество, ед.	Объем, тыс. руб.
Москва	2 154	575 306,4
Санкт-Петербург	2 267	65 865,42
Челябинская область	10	7 197,28
Московская область	12	6 873,44
Вологодская область	3	5 691,67
Приморский край	4	5 649,24
Амурская область	46	3 111
Костромская область	11	2 998,76
Краснодарский край	7	2 821,64
Республика Татарстан	9	2 594,59
Кировская область	13	2 432,34

	Количество, ед.	Объем, тыс. руб.
Республика Коми	4	2 283,09
Владимирская область	3	2 234,4
Свердловская область	5	2 076,51
Нижегородская область	5	2 063,4
Калужская область	3	1 591,85
Республика Дагестан	1	1 500
Новосибирская область	3	1 237,5
Удмуртская Республика	3	1 223,8
Республика Крым	20	1 166,97
Республика Карелия	1	756,49
Саратовская область	2	697,07
Оренбургская область	1	500
Ивановская область	1	440
Тверская область	1	418,67
Иркутская область	2	411,28
Пермский край	3	369
Кемеровская область	1	300
Ставропольский край	1	250
Пензенская область	1	230,5
Рязанская область	3	227,59
Курская область	1	198,5
Самарская область	1	139,6
Калининградская область	1	95
Псковская область	1	26
Томская область	1	15
Чувашская Республика	2	0
Тюменская область	2	0

3. СВЕДЕНИЯ ОБ ИНЦИДЕНТАХ, ПРОИЗОШЕДШИХ ПРИ ЭКСПЛУАТАЦИИ ОПЕРАТОРАМИ ПО ПЕРЕВОДУ ДЕНЕЖНЫХ СРЕДСТВ И ОПЕРАТОРАМИ УСЛУГ ПЛАТЕЖНОЙ ИНФРАСТРУКТУРЫ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В 2019 г. отчитывающиеся операторы направили в Банк России информацию о 973 инцидентах, связанных с несанкционированным доступом к их информационной инфраструктуре, на общую сумму 103,8 млн рублей.

Несанкционированный доступ работников или иных лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры и автоматизированным банковским системам или информации о банковских счетах, стал причиной 877 инцидентов, связанных с переводом денежных средств оператора или его клиентов без их согласия. Объем ущерба в результате таких хищений составил порядка 24,5 млн рублей.

Хищений, произошедших в результате компьютерных атак или несанкционированного доступа к автоматизированным банковским системам (информации о банковских счетах), было зафиксировано в 15 раз меньше – 58 инцидентов, при этом объем хищений составил 23,2 млн рублей.

Несанкционированный доступ работников или иных лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры оператора по переводу денежных средств, к программно-аппаратному обеспечению банкоматов и электронных терминалов стал причиной 14 хищений на сумму порядка 13,5 млн руб., в то время как хищений в результате компьютерных атак и несанкционированного доступа было всего 8 (на сумму около 10,6 млн руб.).

Также в 2019 г. произошли 15 компьютерных атак и два случая несанкционированного доступа к программно-аппаратному обеспечению банкоматов, которые стали причиной несанкционированного снятия денежных средств оператора по переводу денежных средств в банкоматах на сумму 32,2 и 0,9 млн руб. соответственно.

Общая сумма операционных расходов операторов по переводу денежных средств вследствие списаний (снятий) денежных средств в результате несанкционированного доступа к их информационной инфраструктуре составила 27,4 млн рублей.

Указанные объемы хищений денежных средств свидетельствуют о достаточно низкой результативности действий злоумышленников в результате атак на кредитные организации. Это может быть обусловлено повы-

шением внимания операторов к вопросам информационной безопасности, включая проводимую ими работу по данному направлению, а также может быть результатом мероприятий Банка России в области защиты информации при осуществлении переводов денежных средств.

В дальнейшем Банк России планирует уделять достаточное внимание вопросам, связанным с защитой информации в организациях кредитно-финансовой сферы, с целью снижения количества атак на данные организации.

4. СВЕДЕНИЯ О МЕРАХ, ПРИНИМАЕМЫХ БАНКОМ РОССИИ ДЛЯ МИНИМИЗАЦИИ РИСКА ПРОВЕДЕНИЯ ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТОВ

К основным мерам, принимаемым Банком России для минимизации риска проведения операций без согласия клиентов и инцидентов нарушения информационной безопасности при использовании отчитывающимися операторами объектов информационной инфраструктуры, относятся:

- совершенствование законодательства Российской Федерации в области обеспечения информационной безопасности финансовых организаций;
- совершенствование нормативных актов Банка России в области информационной безопасности финансовых организаций;
- повышение финансовой грамотности населения в части обеспечения безопасности применяемых информационных и платежных технологий;
- организация информационного обмена на базе ФинЦЕРТ для осуществления оперативного и непрерывного взаимного информирования об угрозах нарушения информационной безопасности;
- организация информационного обмена на базе ФинЦЕРТ для осуществления оперативного и непрерывного взаимного информирования об операциях без согласия клиентов.

ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОГО ОБМЕНА НА БАЗЕ ФИНЦЕРТ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОПЕРАТИВНОГО И НЕПРЕРЫВНОГО ВЗАИМНОГО ИНФОРМИРОВАНИЯ ОБ ОПЕРАЦИЯХ БЕЗ СОГЛАСИЯ КЛИЕНТОВ

На сегодняшний день законодательство Российской Федерации в области национальной платежной системы устанавливает обязанность для операторов по переводу денежных средств до списания денежных средств со счета отправителя осуществлять проверку операции по переводу денежных средств на предмет ее соответствия признакам операций без согласия. В случае положительного результата проверки оператор по переводу денежных средств обязан приостановить такую операцию, заблокировать ЭСП и связаться со своим клиентом для установления принадлежности операции легальному держателю счета.

Признаки операций без согласия, установленные приказом Банка России № ОД-2525, делятся на две категории: явное соответствие сведениям о получателях и параметрах устройства из базы данных Банка России и отклонение от типовых для клиента значений суммы, времени, места платежа и так далее.

Наличие подобной проверки существенно снижает риск осуществления перевода без согласия клиента. Вместе с тем риск подобной операции остается. В случае если клиент в соответствии с формой, установленной договором, подает обращение о выявлении им операции без согласия, оператор по переводу денежных средств, получивший такое уведомление, должен в срок, не превышающий одного рабочего дня с даты получения обращения, уведомить Банк России о факте операции. Для этого в Банке России на базе АСОИ ФинЦЕРТ развернут прототип АС «Фид-АнтиФрод». Функционал системы позволяет участникам (участники – поднадзорные Банку России организации, что обеспечивает доверие в рамках информационного обмена), в том числе операторам по переводу денежных средств, направлять уведомления посредством как веб-интерфейса в ручном и полуавтоматическом режимах, так и интерфейса автоматической загрузки. В настоящее время соответствующий интерфейс проходит испытания и доступен для тестирования участниками. Формат передаваемых данных установлен стандартом Банка России СТО БР ИББС 1.5, при этом описание интерфейса автоматической загрузки размещено на портале АСОИ ФинЦЕРТ.

При получении Банком России уведомления оператора по переводу денежных средств в автоматическом режиме происходит определение оператора по переводу денежных средств, обслуживающего получателя, после чего в адрес соответствующей организации в автоматизированной системе отправляется уведомление об операции без согласия. При получении такого уведомления оператор по переводу денежных средств в том случае, если отправителем выступает юридическое лицо, в соответствии с требованиями законодательства должен приостановить зачисление денежных средств на расчетный счет получателя и запросить документы, подтверждающие обоснованность платежа. Если платеж уже зачислен, то обратно возвращается статус данного перевода. Вне зависимости от типа заявителя по каждому запросу Банка России по операции без согласия оператор по переводу денежных средств – получатель обязан (в соответствии с нормативным документом Банка России) направить с использованием АСОИ ФинЦЕРТ сведения о получателе (например, зашифрованный номер паспорта).

Учитывая, что АСОИ ФинЦЕРТ работает в автоматическом режиме, сведения об операциях могут направляться и корректно маршрутизироваться независимо от дня недели.

Дополнительно по каждой операции без согласия в рамках промежуточного уведомления оператор по переводу денежных средств, обслуживающий отправителя, имеет возможность на основании сведений, предоставленных клиентом, направить в Банк России информацию о номере обращения клиента в полицию. Таким образом, при должной активности граждан в части защиты своих прав и обращении их в правоохранительные органы в Банке России формируется возможность корреляции фактов обращения граждан в правоохранительные органы по операциям без согласия, сведений о самих операциях и их получателях. Указанную информацию в рамках межведомственного взаимодействия Банк России

может направлять в МВД России для повышения уровня раскрываемости преступлений, в случае когда денежные средства, переводимые в рамках операции без согласия, снимаются получателем.

Следует отметить, что работа по обмену информацией об осуществлении операций без согласия клиентов является сравнительно новым направлением для Банка России. По ее результатам Банк России ставит своей целью налаживание взаимодействия между участниками информационного обмена, сокращение количества и объемов осуществленных операций без согласия клиентов, повышение качества предоставляемых данных по таким операциям. Информирование операторов об операциях без согласия клиентов посредством АСОИ ФинЦЕРТ является каналом оперативного уведомления в отличие от данных, предоставляемых операторами в рамках постоянной отчетности Банка России.

5. ЗАКЛЮЧЕНИЕ

Объем и количество операций, совершенных без согласия клиентов – физических лиц на территории Российской Федерации и за ее пределами с использованием эмитированных российскими банками платежных карт, постоянно увеличиваются. Планомерное развитие дистанционных платежных сервисов и совершенствование национальной платежной системы на основе современных технологий способствуют повышению доступности платежных услуг и расширению сферы безналичных расчетов. Совместная работа Банка России, участников рынка и правоохранительных органов, проведенная в 2018 и 2019 гг. после введения новой формы отчетности 0403203, вступления в силу Федерального закона № 167-ФЗ и запуска АСОИ ФинЦЕРТ и АС «Фид-АнтиФрод» позволила повысить выявляемость несанкционированных операций. Реализация указанных мер обусловила корректировки в ряде наблюдавшихся в предыдущие годы трендов в динамике хищений. Так, количество таких операций за отчетный период составило 571 957 единиц, при этом тенденция 2018 г., связанная с повышением общего объема хищений, в 2019 г. не изменилась. Объем всех операций с использованием ЭСП, совершенных без согласия клиентов, в 2019 г. составил 5723,5 млн рублей. Доля объема операций без согласия клиентов в общем объеме операций, совершенных с использованием платежных карт, в 2019 г. составила 0,0023% (в 2018 г. – 0,0018%). В условиях прогнозируемого дальнейшего роста числа и объема платежей, совершаемых в безналичной форме, Банк России ставит перед собой цель удержать показатель доли операций без согласия клиентов – физических лиц в общем объеме операций, совершенных с использованием платежных карт, ниже уровня 0,005%.

В общем объеме и количестве операций без согласия клиентов – физических лиц основную долю по-прежнему составляют CNP-транзакции: в 2019 г. в общем числе операций их доля составила 65%, в объеме – 52%. На втором месте – 28 и 39% соответственно – операции без согласия клиентов в системе ДБО физических лиц. Однако если средний «чек» по CNP-транзакциям составлял порядка 8 тыс. руб., то в ДБО одно хищение приводило к ущербу в размере в среднем 14 тыс. рублей. Оставшиеся 7% количества и 9% объема операций без согласия клиентов по счетам физических лиц совершались в банкоматах и терминалах (средняя сумма – 13 тыс. руб.).

В качестве причин большей части операций без согласия клиентов (69%) отчитывающимися операторами указываются использование ЭСП без согласия клиента вследствие противоправных действий, потери либо нарушение конфиденциальности аутентификационной информации. Как основание значительной части указанных операций можно отметить воздействие вредоносного кода и побуждение владельца ЭСП к самостоятельному совершению операции путем обмана или злоупотребления доверием.

82% по количеству и 74% по объему операций без согласия клиентов с использованием платежных карт приходится на банки Московского региона. Второе место по количеству занимает Центральный федеральный округ – 11,3%, по объему – Санкт-Петербург (11,5%). На долю операций без согласия клиентов, совершенных за пределами Российской Федерации, приходится 42,5% от количества и 29,3% от объема всех операций без согласия клиентов – физических лиц, совершенных в 2019 году.

В 2019 г. в Банк России была представлена информация о 4609 операциях без согласия клиентов со счетов юридических лиц, совершенных посредством системы ДБО, на общую сумму 701 млн рублей. Основное количество указанных операций приходится на сегмент от 100 тыс. до 10 млн руб., при этом средняя сумма такой операции составляла порядка 152 тыс. рублей. Почти половина (49,2%) приходится на Санкт-Петербург, при этом банки Московского региона с отрывом лидируют по объему хищений, который составляет 82% от общего по России. Они же находятся на втором месте по количеству хищений.

За отчетный период отчитывающиеся операторы направили в Банк России информацию о 956 переводах принадлежащих им или находящихся на корреспондентских счетах их клиентов денежных средств без их согласия на сумму 71,5 млн рублей. Еще 32,3 млн руб. – средств банков или их клиентов – было снято в банкоматах в результате 17 инцидентов, связанных с несанкционированным доступом работников оператора по переводу денежных средств или иных лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры оператора по переводу денежных средств, к программно-аппаратному обеспечению банкоматов либо с компьютерными атаками.

Растущая доступность платежных услуг, осуществляемых посредством сети Интернет, приводит к смещению интереса злоумышленников (поступательно за вектором интересов клиентов кредитных организаций) от банкоматов и организаций торговли в сторону CNP-транзакций, каналов ДБО. С учетом развития финансовых услуг, совершаемых через сеть Интернет без предоставления карты, мы прогнозируем сохранение восходящего тренда миграции операций без согласия клиентов в CNP-среду. Активно использовавшаяся злоумышленниками в 2019 г. технология подмены телефонных номеров также, скорее всего, останется одним из главных инструментов обмана граждан.

К основным необходимым мерам, направленным на снижение риска хищений, следует отнести внедрение технологий, связанных с подтверждением операции по альтернативному каналу связи, а также дальнейшее развитие антифрод-систем, в том числе более широкий охват указанными системами каналов проведения операций, включая ДБО, СМС-банкинг. Немаловажным фактором борьбы с несанкционированными операциями может стать внедрение антивирусного программного обеспечения в банковские приложения, устанавливаемые на устройства клиента, а также более точных систем и методов аутентификации клиента.

Применение антифрод-систем на сегодняшний день получило нормативное закрепление в рамках изменений в Федеральный закон № 161-ФЗ, внесенных Федеральным законом № 167-ФЗ.

К дополнительным мерам противодействия CNP-транзакциям без согласия клиентов необходимо отнести взаимодействие организаций кредитно-финансовой сферы с регистраторами доменных имен в части доведения с использованием АСОИ сведений о фишинговых ресурсах (домены, с которых осуществляются мошеннические действия, связанные с использованием платежных карт).

Банки возместили клиентам 935 млн руб. (15%, или каждый 7-й похищенный рубль). Текущий уровень возмещения объясняется высокой долей социальной инженерии среди операций без согласия клиентов, которые в результате обмана или злоупотребления доверием нарушают условия договора с кредитными организациями, предусматривающие необходимость сохранения конфиденциальности платежной информации. В связи с этим Банк России намерен рассмотреть возможность изменения процедуры возврата (компенсации) похищенных средств клиентов.