Банк России

ОБЗОР ОПЕРАЦИЙ, СОВЕРШЕННЫХ БЕЗ СОГЛАСИЯ КЛИЕНТОВ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ ЗА 2020 ГОД

Москва
2021

СОДЕРЖАНИЕ

Материал подготовлен Департаментом 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»
ДБО	Дистанционное банковское обслуживание
Комплекс БР ИББС	Комплекс документов Банка России по стандартизации обеспечения информационной безопасности организаций банковской системы Российской Федерации, описывающих 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 клиента	Операции по переводу денежных средств, соответствующие утвержденным приказом Банка России от 27 сентября 2018 года № ОД-2525 признакам осуществления перевода денежных средств без согласия клиента
Положение Банка России № 382-П	Положение Банка России от 09.06.2012 № 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 09.06.2012 № 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 24.11.2016 № 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

Мониторинг и анализ операций, совершаемых без согласия клиентов кредитных и некредитных финансовых организаций, является задачей Банка России с 2015 года. Получаемые от участников информационного обмена данные о признаках и структуре указанных операций формируют базу знаний, использование которой позволяет банкам оперативно выявлять и предотвращать новые покушения на хищение средств клиентов организаций кредитно-финансовой сферы.

Информационный обмен ведется посредством Автоматизированной системы обработки инцидентов (АСОИ ФинЦЕРТ). Ее использование позволяет существенно облегчить участникам информационного обмена выполнение требований действующего законодательства и нормативных актов Банка России в отношении обеспечения безопасности банковских операций.

В 2019 году на базе АСОИ ФинЦЕРТ была введена в действие система «Фид-АнтиФрод», предназначенная для аккумулирования и быстрого обмена информацией об операциях без согласия клиента. Участники информационного обмена передают данные о подозрительной операции в ФинЦЕРТ, который оперативно информирует с помощью указанных систем кредитные организации, являющиеся получателями денежных средств. После этого ФинЦЕРТ анализирует информацию по таким операциям и формирует сообщения, содержащие признаки операций, совершенных без согласия клиента (так называемые фиды), и предназначенные для всех кредитных организаций. Таким образом, данные из АС «Фид-АнтиФрод» позволяют кредитным организациям дополнять свои антифрод-системы информацией, получаемой от других банков, уже столкнувшихся с мошенниками. Это существенно повышает эффективность работы по предотвращению операций без согласия клиента.

По состоянию на декабрь 2020 года накоплено более 43 тыс. уникальных признаков операций, совершенных без согласия клиента (в том числе 23 444 карт, 12 637 хэшей паспортов, 4723 телефонов, 1237 счетов, 1100 электронных кошельков, 266 ИНН).

В настоящем обзоре приведены данные о количестве и объеме операций, совершенных без согласия клиента, за 2020 год. Обзор составлен на основе сведений, предоставленных отчитывающимися операторами по переводу денежных средств и операторами услуг платежной инфраструктуры в Банк России в рамках формы отчетности 0403203.

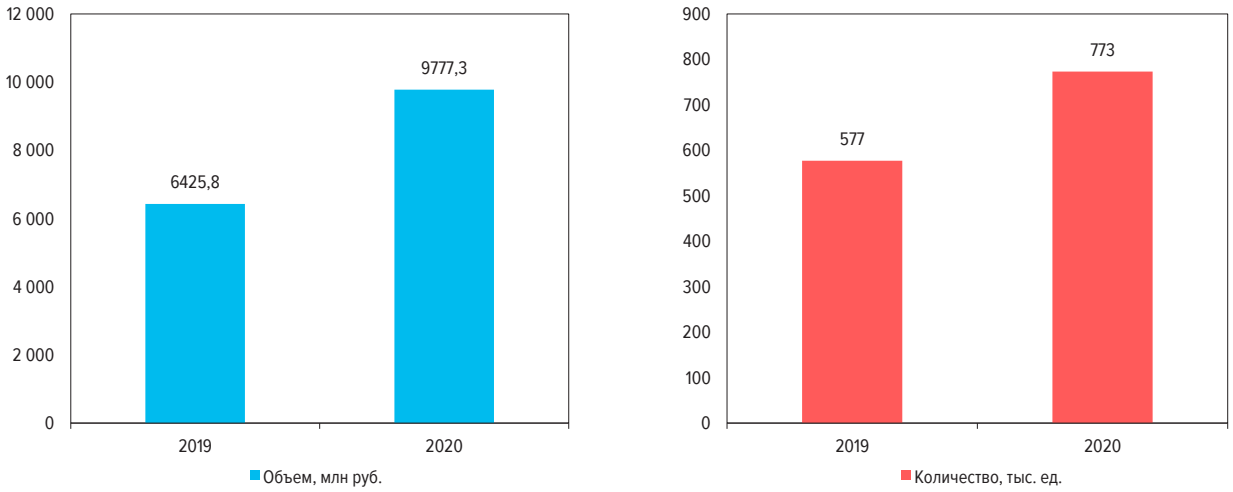
Настоящий обзор может быть использован операторами по переводу денежных средств, а также операторами услуг платежной инфраструктуры в целях планирования мероприятий по управлению рисками, внутреннему контролю, защите информации, в том числе в целях учета количества и характера инцидентов, произошедших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

1. ОБЩИЕ СВЕДЕНИЯ ОБ ОПЕРАЦИЯХ БЕЗ СОГЛАСИЯ КЛИЕНТА

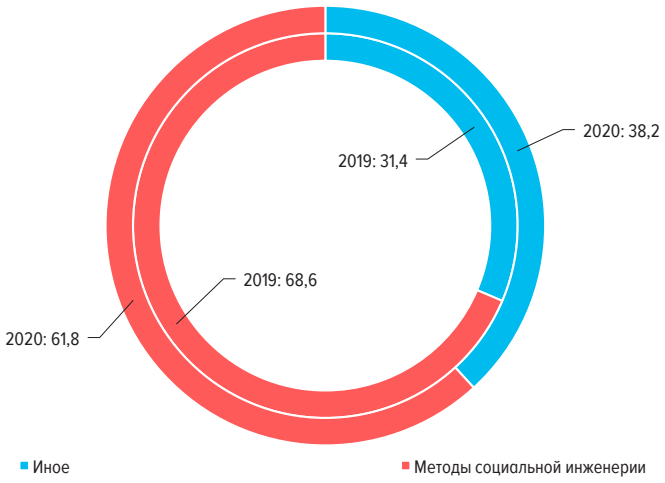
В 2020 году количество и объем операций по переводу денежных средств с использованием электронных средств платежа (ЭСП) физических лиц составили 49,6 млрд единиц и 91,08 трлн руб., увеличившись по сравнению с 2019 годом на 23,1 и 28,2% соответственно. При этом количество операций без согласия клиента увеличилось на 34,0% (773 008 операций за 2020 год против 576 897 операций за 2019 год). Объем таких операций вырос на 52,2%, составив 9777,3 млн руб. (за аналогичный период 2019 года – 6425,8 млн руб.).

Общая доля операций без согласия, совершенных с использованием приемов и методов социальной инженерии, снизилась с 68,6 до 61,8%. Изменение доли операций без согласия клиента, совершенных с применением методов социальной инженерии, характеризует эффективность работы Банка России с кредитными организациями и населением по повышению осведомленности клиентов банков о правилах безопасного использования электронных средств платежа.

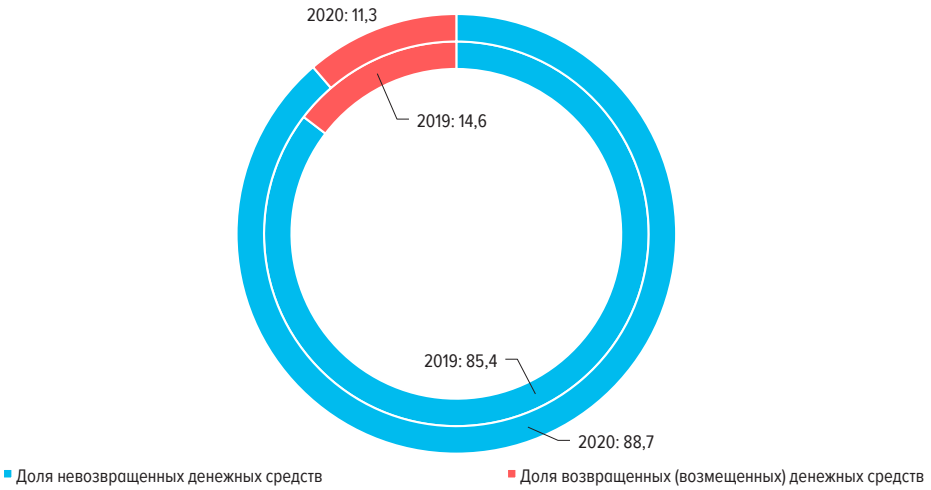
ДИНАМИКА КОЛИЧЕСТВА И ОБЪЕМА ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТА *Рис. 1*



ПРИЧИНЫ СОВЕРШЕНИЯ ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТА *Рис. 2*
(%)



РАСПРЕДЕЛЕНИЕ ВОЗВРАЩЕНИЯ (ВОЗМЕЩЕНИЯ) ДЕНЕЖНЫХ СРЕДСТВ *Рис. 3*
(%)



Средняя сумма одной операции без согласия клиента по счетам физических лиц в 2020 году составила 11,4 тыс. руб., юридических лиц – 347,8 тыс. рублей. При этом для клиентов – физических лиц средняя сумма операции с использованием системы дистанционного банковского обслуживания (ДБО) составила 27,8 тыс. руб., операций посредством банкоматов и платежных терминалов – 15,2 тыс. руб., CNP-операции – 7,2 тыс. рублей. Указанная тенденция далее будет раскрыта более подробно.

Согласно имеющейся у Банка России статистике, клиентам кредитных организаций в 2020 году вернули (возместили) 11,3% (1104,6 млн руб.) от всего объема операций по переводу денежных средств, совершенных без согласия клиента (в 2019 году – 14,6%, или 935,9 млн руб.). Такой уровень данного показателя обусловлен существующими договорными отношениями кредитных организаций со своими клиентами. Кредитные организации не возвращают денежные средства в случае нарушения клиентом условий договора, предусматривающих необходимость сохранения конфиденциальности платежной информации (статья 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе»).

2. СВЕДЕНИЯ ОБ ОПЕРАЦИЯХ БЕЗ СОГЛАСИЯ КЛИЕНТОВ – ФИЗИЧЕСКИХ ЛИЦ

Динамика количества и объема операций с использованием ЭСП (включая платежные карты)

По данным Банка России, количество и объем операций физических лиц по переводу денежных средств с использованием ЭСП в 2020 году составили 49,6 млрд единиц и 91,08 трлн руб. соответственно (годом ранее – 40,3 млрд единиц и 71,03 трлн руб.). 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 клиента

Показатели количества и объема операций без согласия клиентов – физических лиц в данном обзоре приводятся в соответствии с данными формы отчетности 0403203.

Объем всех операций, совершенных без согласия клиента с использованием ЭСП, в 2020 году составил 8757,2 млн рублей. Количество таких операций – 770 075 единиц.

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

- операции через банкоматы, терминалы и импринтеры;
- оплата товаров и услуг в Интернете (CNP-транзакции);
- операции в системе ДБО.

Необходимо отметить, что большая часть операций без согласия клиента совершается в результате использования злоумышленниками методов социальной инженерии (введение в заблуждение путем обмана или злоупотребления доверием) для получения несанкционированного прямого доступа к ЭСП владельцев средств либо побуждения их самостоятельно совершить перевод в пользу мошенников.

Доля операций без согласия клиента в общем объеме операций, совершенных с использованием платежных карт

За 2020 год доля операций без согласия клиента в общем объеме операций по переводу денежных средств составила 0,00117% (в 2019 году – 0,00089%). 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%.

Динамика отмеченного показателя, наблюдаемого с 2015 года, подтвердила обоснованность принятых мер по повышению прозрачности представляемых банками данных, правильность разработки и внедрения мер по минимизации риска осуществления операций без со-

гласия клиента, принимаемых участниками рынка и Банком России, а также необходимость их дальнейшего развития. Текущий показатель доли операций без согласия клиента в общем объеме операций по переводу денежных средств учитывает не только несанкционированные операции с использованием платежных карт, но и операции без согласия клиента, совершаемые с использованием иных электронных средств платежа.

Распределение по условиям совершения операций без согласия клиента

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.

В 2020 году было зафиксировано 48,7 тыс. случаев использования платежных карт (за исключением предоплаченных) без согласия их владельцев в банкомате или терминале. Из них 15,8% операций проведены в результате использования злоумышленниками приемов социальной инженерии. Общая сумма ущерба по хищениям через банкоматы и терминалы выросла на 40,3% по сравнению с аналогичным показателем 2019 года и составила свыше 740,4 млн руб., при этом банки вернули клиентам 9,0% похищенных средств (66,4 млн руб.). В 2019 году было отмечено 40,1 тыс. случаев использования платежных карт (за исключением предоплаченных) без согласия их владельцев в банкомате или терминале на общую сумму 527,9 млн руб., при этом банки вернули клиентами 10,4% похищенных средств (54,8 млн руб.).

Как и годом ранее, 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 585,3 тыс. таких транзакций, 61,5% из которых (359,7 тыс. транзакций) – результат применения методов социальной инженерии. Сумма ущерба составила 4229,1 млн руб., при этом банки возместили клиентам 19,2% всех похищенных денежных средств (всего 813,4 млн руб.). В 2019 году было зафиксировано 371,2 тыс. таких операций на общую сумму 2969,9 млн руб., а доля возвращенных денежных средств составила 22,0% (653,9 млн руб.).

Системы ДБО физических лиц становились мишенью мошенников 136,1 тыс. раз, однако доля социальной инженерии в их общем числе самая высокая – порядка 80%. 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 3787,6 млн руб., что выше аналогичного показателя 2019 года на 70,1% (в 2019 году – около 2227,0 млн руб.). При этом банки вернули клиентам всего 136,5 млн руб. (в 2019 году – 162,3 млн руб.).

Распределение по причинам совершения операций без согласия клиента

Как и годом ранее, в качестве причины подавляющего большинства хищений отчитывающиеся операторы указывают социальную инженерию.

По итогам 2020 года ее доля составила 61,8% случаев (в 2019 году – 68,6%).

Данное снижение может объясняться 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 несоблюдения правил информационной безопасности и цифровой гигиены 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. Это является важным источником информации для формирования понимания типа операций, вызывающих повышенный интерес злоумышленников, с учетом бизнес-стратегии организации. В дальнейшем знание востребованных типов операций позволит операторам 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.

Успешность применения методов социальной инженерии обусловлена в том числе нелегальным оборотом персональных данных, которые используются для организации массовых звонков клиентам кредитных организаций. Необходимо подчеркнуть, что источниками таких данных в большинстве случаев являются не столько кредитные организации, сколько иные операторы – торгово-сервисные предприятия, некоммерческие организации и так далее.

Реализовать успешную атаку несложно: достаточно иметь немного информации о клиенте кредитной организации (например, ФИО и номер телефона). Злоумышленники приобретают базы данных, содержащие персональные данные клиентов, и осуществляют звонок клиенту кредитной организации якобы от имени сотрудника финансовой организации:

- под предлогом остановки операции, совершаемой без согласия клиента, злоумышленники выпытывают у жертвы данные карт, коды из СМС-сообщений и другую информацию, необходимую для хищения средств;
- сообщают об ошибочном переводе денежных средств, просят снять деньги в банкомате и после этого перевести их на безопасный, по заявлениям злоумышленников, счет кредитной организации;
- сообщают о компрометации личного кабинета системы ДБО, под предлогом безопасной смены пароля просят продиктовать код из СМС, необходимый для входа в личный кабинет, для совершения хищения средств;
- под предлогом компрометации мобильного устройства просят установить на телефон якобы безопасное приложение, которое впоследствии позволит злоумышленнику удаленно подключиться к мобильному телефону жертвы и совершить хищение средств.

После успешного перевода денежных средств со счета клиента злоумышленники обычно снимают похищенные денежные средства за очень короткий промежуток времени.

Следует отметить, что основным каналом совершения операций по переводу денежных средств без согласия клиента является сеть Интернет. Наряду со схемами хищений, имитирующими онлайн-оплату товаров и услуг, а также использующими вывод средств со счетов через системы ДБО, в 2020 году Департамент информационной безопасности Банка России отметил значительный рост числа инцидентов, связанных с хищением кредитных денежных средств, оформленных мошенниками от имени клиента на их имя посредством удаленных каналов обслуживания.

Успешная реализация таких атак приводит к хищению у клиентов не только собственных, но и кредитных денежных средств, за использование которых кредитная организация в соответствии с условиями договора начисляет проценты.

3. СВЕДЕНИЯ ОБ ОПЕРАЦИЯХ БЕЗ СОГЛАСИЯ КЛИЕНТА СО СЧЕТОВ ЮРИДИЧЕСКИХ ЛИЦ

Динамика количества и объема операций без согласия клиента

В настоящем обзоре под операциями без согласия клиента 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 году юридические лица сообщили в банки о 4609 операциях без согласия на общую сумму 701,0 млн рублей. В прошедшем году объем таких операций вырос на 45,5% по сравнению с 2019 годом и составил 1020 млн руб., а количество операций снизилось на 36,4%, до 2933.

Порядка 8,7% похищенных средств (88,4 млн руб.) компенсированы либо возвращены пострадавшим организациям. При этом в 2019 году объем возвращенных (возмещенных) денежных средств составил 64,9 млн руб., что составило 9,3% от похищенных денежных средств.

Распределение по причинам совершения операций без согласия клиента

Данные, представленные отчитывающимися операторами, свидетельствуют о том, что операции без согласия клиентов – юридических лиц происходили в результате воздействия социальной инженерии в 33% случаев (980 хищений). К ним относятся в первую очередь инциденты, связанные с получением злоумышленниками доступа к системе ДБО с использованием вредоносного программного обеспечения, рассчитанного на взлом программного обеспечения стационарных компьютеров. Полагаем, что проблема останется актуальной и в 2021 году. В виде рекомендаций следует указать необходимость повышения качества работы отчитывающихся операторов в области осведомления клиентов в вопросах киберграмотности.

Средняя сумма одной операции без согласия клиента по счетам физических лиц в 2020 году составила 11,4 тыс. руб., юридических лиц – 347,8 тыс. рублей. Если для осуществления операции без согласия клиента с использованием платежной карты злоумышленники вынуждены учитывать максимальные размеры суммы операции (лимиты на операции со счета, установленные банком или клиентом), то для операций без согласия со счетов юридических лиц характерна особенность в виде больших сумм каждой операции в отдельности. При проведении подобной операции со счетов юридических лиц злоумышленники для успешного ее осуществления в лучшем случае вынуждены имитировать модель операций юридического лица, а в худшем – ограничены только количеством денежных средств на банковском счете юридического лица.

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

В 2020 году отчитывающиеся операторы направили в Банк России информацию о 581 инциденте, связанном с несанкционированным доступом к их информационной инфраструктуре, на общую сумму порядка 46 млн рублей. При этом в 2019 году количество таких инцидентов составило 973 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 443 инцидентов, связанных с переводом денежных средств оператора или его клиентов без их согласия. Объем ущерба в результате таких хищений составил порядка 9 млн руб. (в 2019 году – 877 инцидентов на общую сумму 24,5 млн руб.).

В 2020 году было зафиксировано 130 случаев хищения, произошедших в результате компьютерных атак или несанкционированного доступа к автоматизированным банковским системам (информации о банковских счетах), при этом сумма хищений составила практически 32 млн рублей. В 2019 году таких случаев было значительно меньше – 58 инцидентов, однако общая сумма была меньше на 8,8 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 двух хищений на сумму порядка 1 млн руб., в то время как хищений в результате компьютерных атак и несанкционированного доступа зафиксировано не было.

Также в 2020 году произошли четыре компьютерные атаки 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 2,8 и 1,2 млн руб. соответственно. В 2019 году произошли 15 компьютерных атак и два случая несанкционированного доступа к программно-аппаратному обеспечению банкоматов, общая сумма ущерба составила 33,1 млн рублей.

Общая сумма операционных расходов операторов по переводу денежных средств вследствие списаний (снятий) денежных средств в результате несанкционированного доступа к их информационной инфраструктуре в 2020 году составила 8,1 млн руб. (в 2019 году – 27,4 млн руб.).

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

В дальнейшем Банк России планирует продолжать уделять достаточное внимание вопросам, связанным с защитой информации в организациях кредитно-финансовой сферы, с целью снижения количества результативных атак на данные организации, а также минимизации возможностей несанкционированного доступа сотрудников к информационным системам банков и последствий такого доступа.

5. СВЕДЕНИЯ О МЕРАХ, ПРИНИМАЕМЫХ БАНКОМ РОССИИ ДЛЯ МИНИМИЗАЦИИ РИСКА ПРОВЕДЕНИЯ ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТА

К основным мерам, принимаемым Банком России для минимизации риска проведения операций без согласия клиента и реализации 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.

В 2021 году Банк России продолжает работу по противодействию операциям без согласия клиента в рамках проработки нормативных инициатив по следующим направлениям:

- борьба с нелегальным оборотом персональных данных;
- создание стимулов для банков в направлении повышения качества антифрод-процедур;
- создание условий для повышения эффективности деятельности правоохранительных органов;
- расширение аудитории программ киберграмотности, ориентированных на целевые группы клиентов – физических лиц, с целью доведения информации до каждого клиента – физического лица.

Организация информационного обмена на базе ФинЦЕРТ для осуществления оперативного и непрерывного взаимного информирования об операциях без согласия клиента

В рамках взаимодействия с кредитно-финансовыми организациями Банк России проводит работу по противодействию хищению денежных средств со счетов клиентов организаций кредитно-финансовой сферы. В целях реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента операторы по переводу денежных средств, операторы платежных систем, операторы услуг платежной инфраструктуры (далее – субъекты НПС) направляют в Банк России информацию обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента. В свою очередь Банк России осуществляет формирование и ведение базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, информацию из которой субъекты НПС вправе получать от Банка России, в том числе для реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента, в порядке, установленном Банком России, а также для повышения эффективности функционирования применяемых ими антифрод-систем.

Оператор по переводу денежных средств в рамках реализуемой им системы управления рисками определяет в документах, регламентирующих процедуры управления рисками, процедуры выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, на основе анализа характера, параметров и объема совершаемых его клиентами операций (осуществляемой клиентами деятельности).

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 о случаях и попытках осуществления переводов денежных средств без согласия клиента 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. При этом вся необходимая для участников информационного обмена информация размещена 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 информация о статусе 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.

В целях обеспечения защиты информации при переводах денежных средств Банк России осуществляет формирование и ведение базы данных о случаях и попытках проведения переводов денежных средств без согласия клиента.

Операторы по переводу денежных средств, операторы платежных систем, операторы услуг платежной инфраструктуры могут направлять в Банк России следующую информацию, которая формирует указанную базу:

- о результате вычисления специального кода номера документа, удостоверяющего личность получателя средств;
- о результате вычисления специального кода страхового номера индивидуального лицевого счета застрахованного лица в системе персонифицированного учета Пенсионного фонда Российской Федерации получателя средств (СНИЛС);
- о номере платежной карты получателя средств;
- о номере банковского счета получателя средств, открытого у оператора по переводу денежных средств, обслуживающего получателя средств;

- об абонентском номере подвижной радиотелефонной связи получателя средств;
- о номере и наименовании электронного кошелька получателя средств.

Вся перечисленная информация хранится в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента в обезличенном виде.

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 Банк России имеет возможность анализировать факты обращений граждан в правоохранительные органы по операциям без согласия, сведений о самих операциях и их получателях. Полученную по результатам анализа 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.

ЗАКЛЮЧЕНИЕ

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 2018–2020 годах 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 773 008 единиц, при этом тенденция 2019 года, связанная с повышением общего объема хищений, в 2020 году не изменилась. Объем всех операций с использованием ЭСП, совершенных без согласия клиента, в 2020 году составил 9777,3 млн рублей. Доля операций без согласия клиента в общем объеме операций по переводу денежных средств в 2020 году составила 0,00117% (в 2019 году – 0,00089%). 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 клиента в общем объеме операций по переводу денежных средств ниже уровня 0,005%.

В общем объеме и количестве операций без согласия клиентов – физических лиц основную долю по-прежнему составляют CNP-транзакции: в 2020 году в общем числе операций их доля составила 76,0%, в общем объеме – 48,3%. На втором месте – 17,7 и 43,2% соответственно – операции без согласия клиента в системе ДБО физических лиц. Однако если средний «чек» по CNP-транзакциям составлял порядка 7,2 тыс. руб., то в ДБО одно хищение приводило к ущербу в размере в среднем 27,8 тыс. рублей. Оставшиеся 6,3% количества и 8,5% объема операций без согласия клиента по счетам физических лиц совершались через банкоматы и терминалы (средняя сумма – 15,2 тыс. руб.).

В качестве причин большей части операций без согласия клиента (61,8%) отчитывающимися операторами указываются использование ЭСП без согласия клиента вследствие противоправных действий, потери либо нарушения конфиденциальности аутентификационной информации. Как основания значительной части указанных операций можно отметить воздействие вредоносного кода и побуждение владельца ЭСП к самостоятельному совершению операции путем обмана или злоупотребления доверием.

В 2020 году в Банк России была представлена информация о 2933 операциях без согласия клиента со счетов юридических лиц, совершенных посредством системы ДБО, на общую сумму 1020,0 млн рублей. При этом средняя сумма такой операции составляла порядка 347,8 тыс. рублей.

За отчетный период операторы направили в Банк России информацию о 575 переводах принадлежащих им или находящихся на корреспондентских счетах их клиентов денежных средств без их согласия на сумму 42 млн рублей. Еще практически 4 млн руб. средств банков или их клиентов было снято в банкомате в результате шести 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, предоставляемых 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, Банк России прогнозирует сохранение восходящего тренда миграции операций без согласия клиента в CNP-среду.

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 клиента необходимо отнести взаимодействие организаций кредитно-финансовой сферы с регистраторами доменных имен в части доведения с использованием АСОИ ФинЦЕРТ сведений о фишинговых ресурсах (домены, с которых осуществляются мошеннические действия, связанные с использованием платежных карт).

В 2020 году банки возместили клиентам – физическим лицам 1104,6 млн руб. (11,3%). Текущий уровень возмещения объясняется высокой долей социальной инженерии среди операций без согласия клиентов, которые под действием 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.