

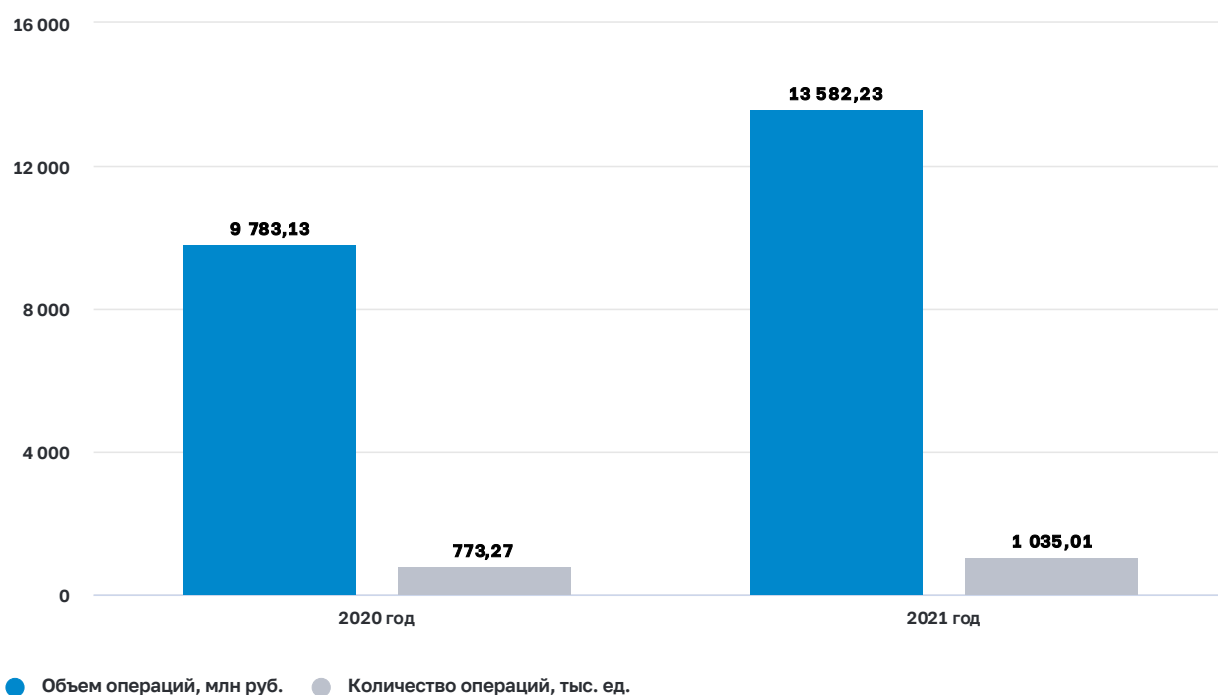
Обзор операций, совершенных без согласия клиентов финансовых организаций в 2021 году

11 апреля 2022 года

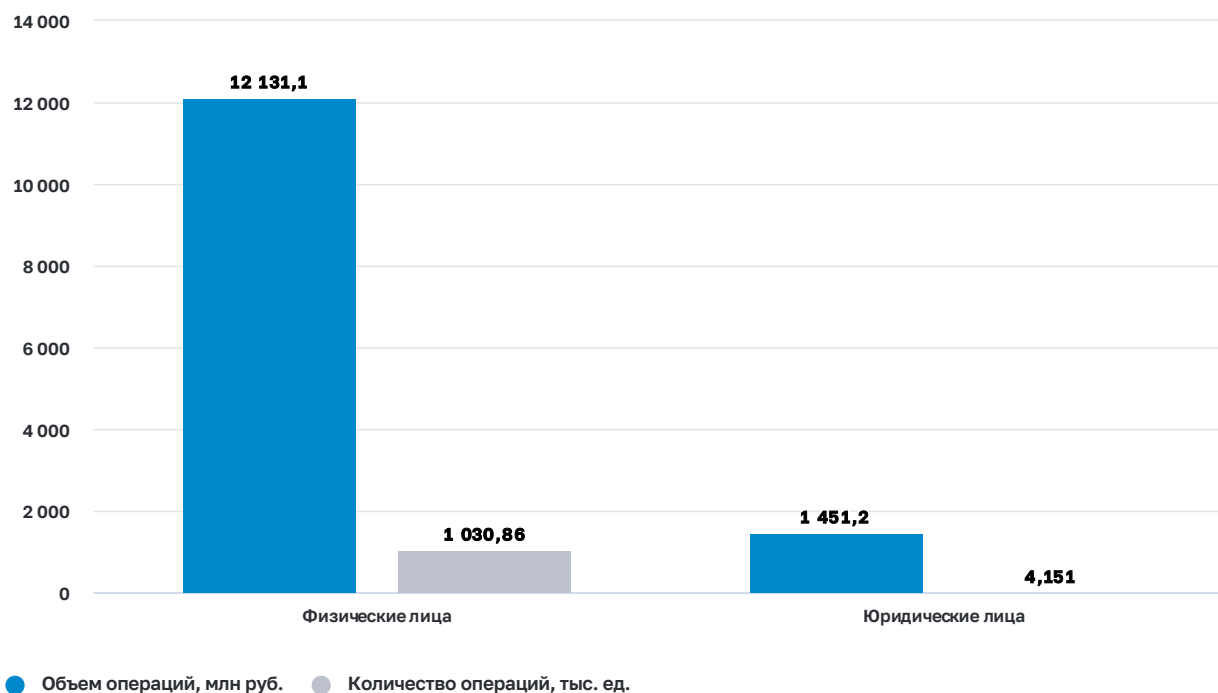
1. Общие сведения об операциях без согласия клиентов¹

В 2021 году количество и объем операций без согласия клиентов увеличились по сравнению с 2020 годом на 33,8 и 38,8% соответственно на фоне активного развития новых дистанционных платежных сервисов и роста объема денежных переводов (+28%, до 1 048,4 трлн руб) с использованием электронных средств платежа (платежные карты и иные электронные средства платежа). В 2021 году доля объема операций без согласия клиентов в общем объеме операций по переводу денежных средств составила 0,00130% (в 2020 году – 0,00120%)¹. Эти значения не превышают установленный Банком России целевой показатель доли таких операций в общем объеме операций (0,005%), совершенных с использованием платежных карт.

Общий объем и количество операций без согласия клиентов



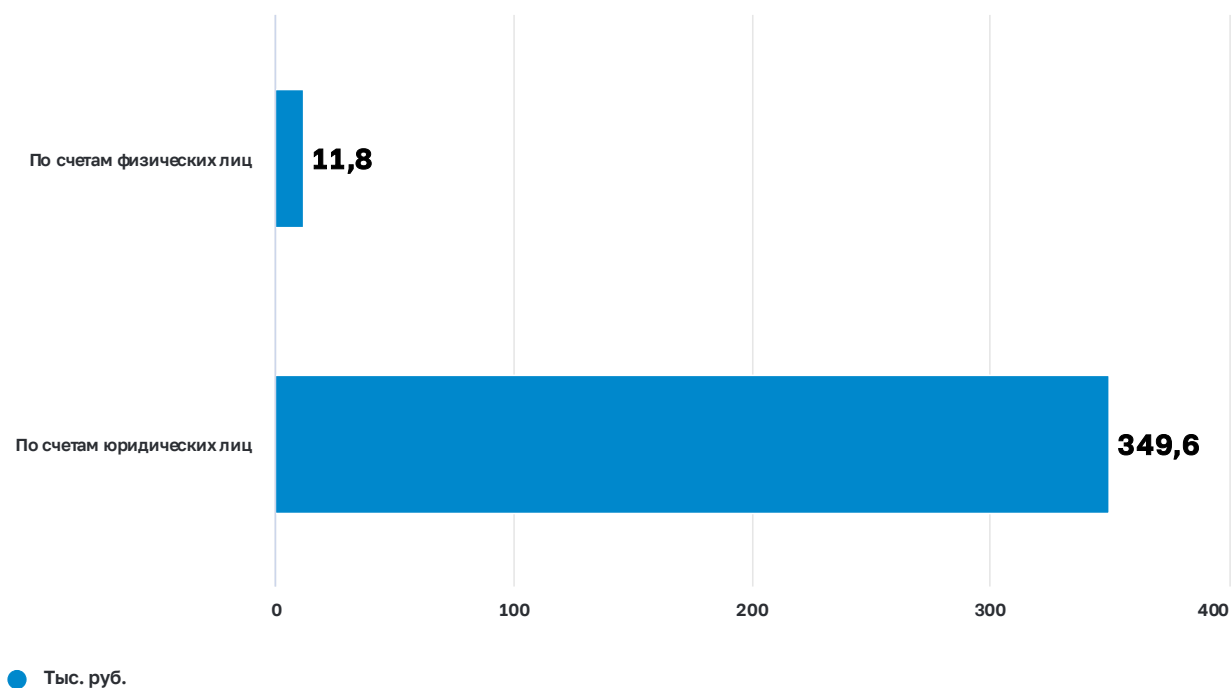
Динамика операций без согласия клиентов: физические и юридические лица



Показатели операций без согласия клиентов

Основным инструментом злоумышленников для хищения средств осталось использование приемов и методов социальной инженерии, когда человек под психологическим воздействием добровольно переводит денежные средства или раскрывает банковские сведения, позволяющие злоумышленникам совершить хищение. Доля таких операций снизилась с 61,8 до 49,4%². По оценке Банка России, в 2021 году наблюдался рост средней суммы одного хищения, совершенного с использованием приемов и методов социальной инженерии, что в том числе привело к увеличению общего размера ущерба по операциям без согласия клиентов. В 2021 году клиентам кредитных организаций возвратили 6,8% (920,5 млн руб.) от всего объема операций по переводу денежных средств, совершенных без согласия клиентов (в 2020 году данный показатель составил 11,3%, или 1 105,3 млн руб.).

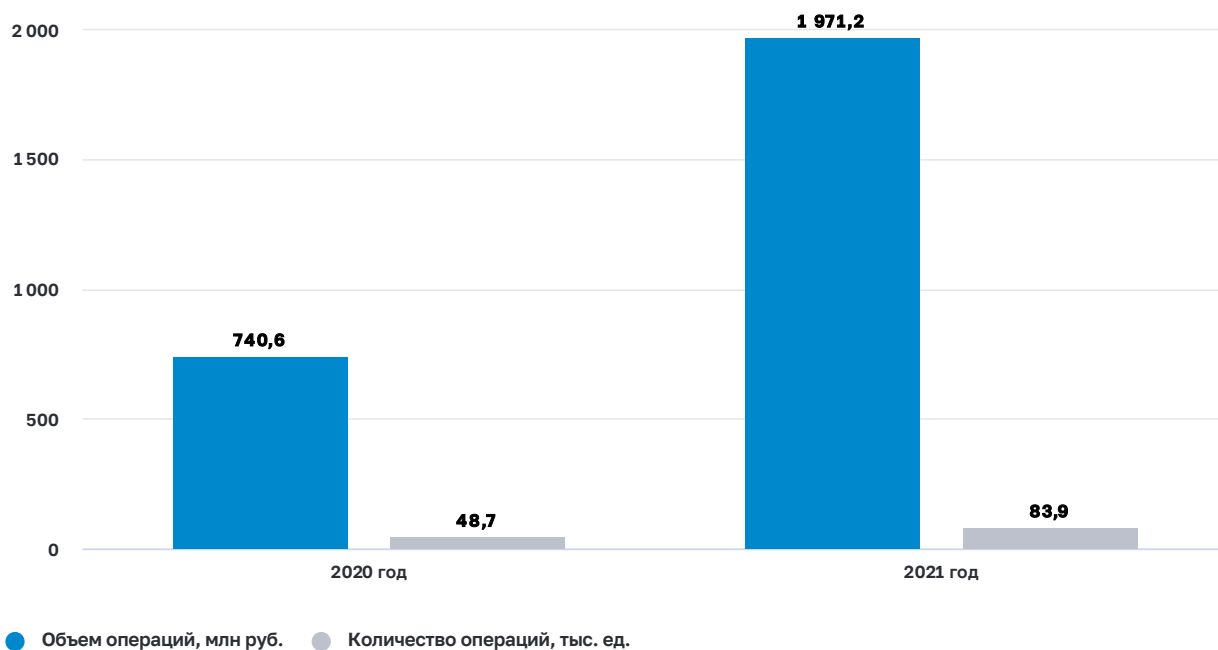
Средняя сумма одной операции без согласия клиента



Распределение по условиям совершения операций без согласия клиентов – физических лиц

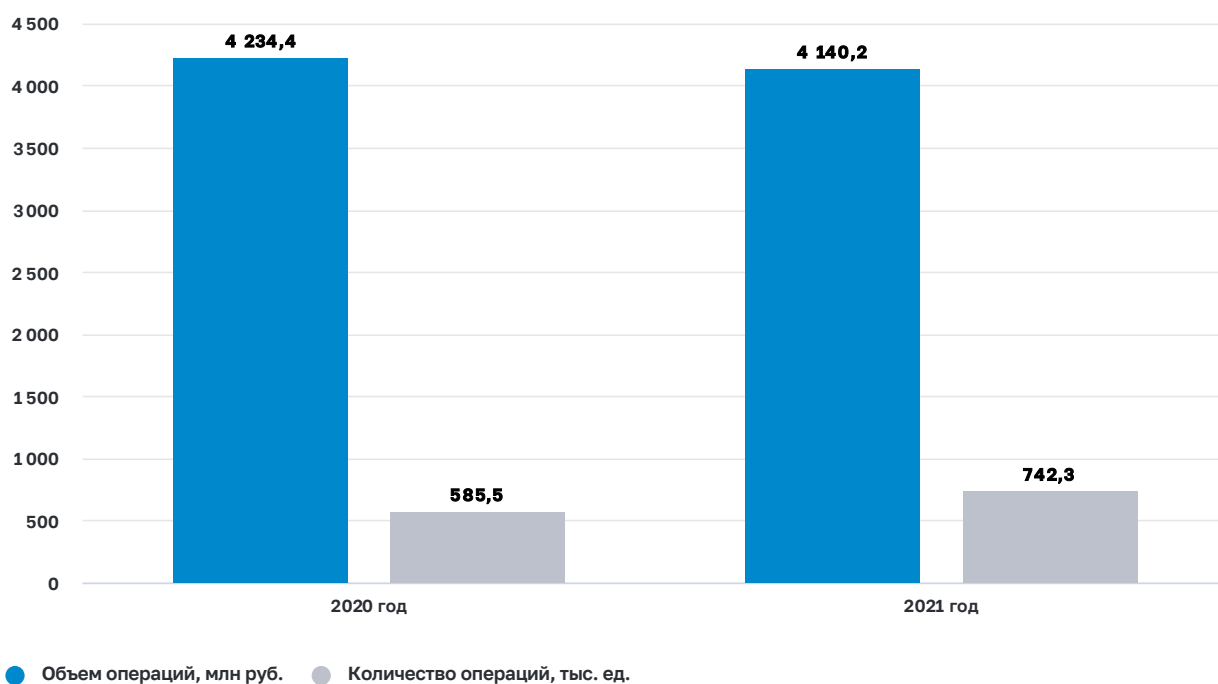
В 2021 году зафиксировано 83,9 тыс. случаев использования платежных карт (за исключением предоплаченных) без согласия их владельцев в банкоматах или терминалах на общую сумму 1 971,2 млн руб., из которых 22,5% операций произошло в результате использования злоумышленниками приемов и методов социальной инженерии. Злоумышленники активно применяли комбинированные схемы мошенничества, при которых жертву вынуждали совершать перевод через этот канал, что привело к росту показателя операций без согласия клиентов в этой группе. Средняя сумма одной операции без согласия клиента составила 23,5 тыс. рублей.

Операции без согласия клиентов в банкоматах, терминалах, импринтерах



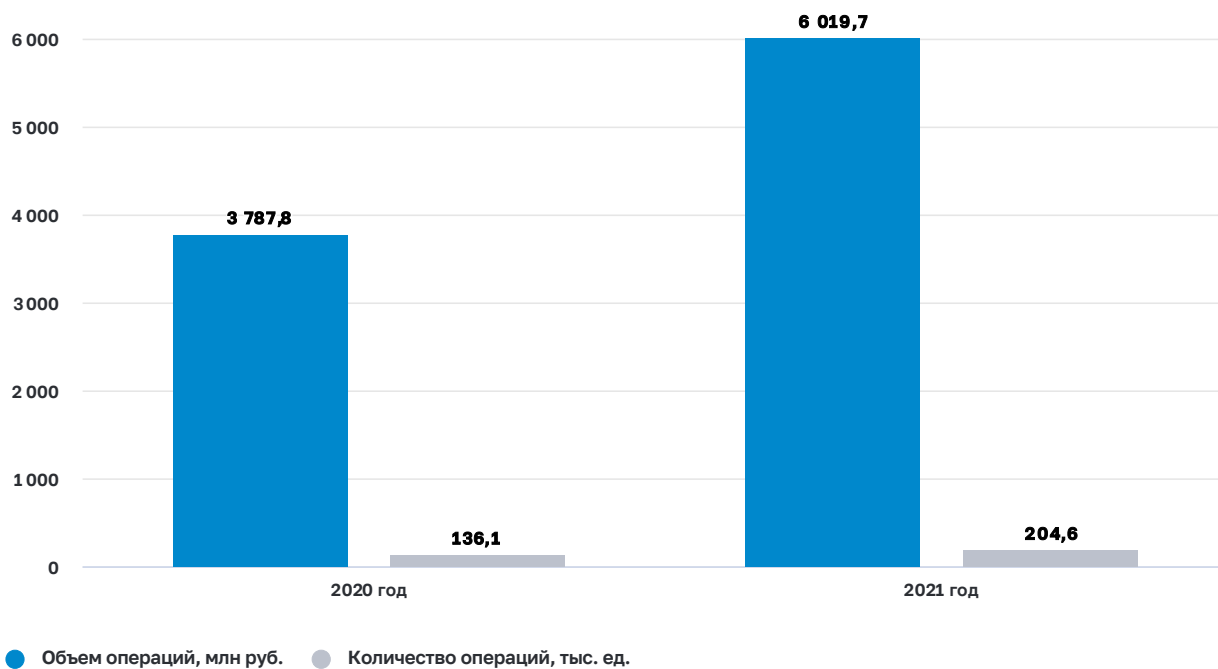
Больше всего операций без согласия клиентов — физических лиц пришлось на CNP-транзакции. Клиенты банков сообщили в 2021 году о 742,3 тыс. таких транзакций, 44,5% из которых — результат применения к ним приемов и методов социальной инженерии. Объем хищений составил 4 140,2 млн руб., средняя сумма одной операции без согласия клиента — 5,6 тыс. рублей.

Операции без согласия клиентов при оплате товаров и услуг в Интернете (CNP-транзакции)



Системы ДБО физических лиц становились мишенью мошенников более 204,6 тыс. раз, доля социальной инженерии составила 78,0%. Объем хищений составил 6 019,7 млн руб., средняя сумма одной операции без согласия клиента – 29,4 тыс. рублей.

Операции без согласия клиентов в дистанционном банковском обслуживании



2. Статистические данные АСОИ ФинЦЕРТ

Атаки с использованием телефонного мошенничества

В 2021 году Банк России инициировал блокировку 179 071 номера телефонов, используемых злоумышленниками для хищения средств у граждан.

Мошеннические телефонные номера (ед.)

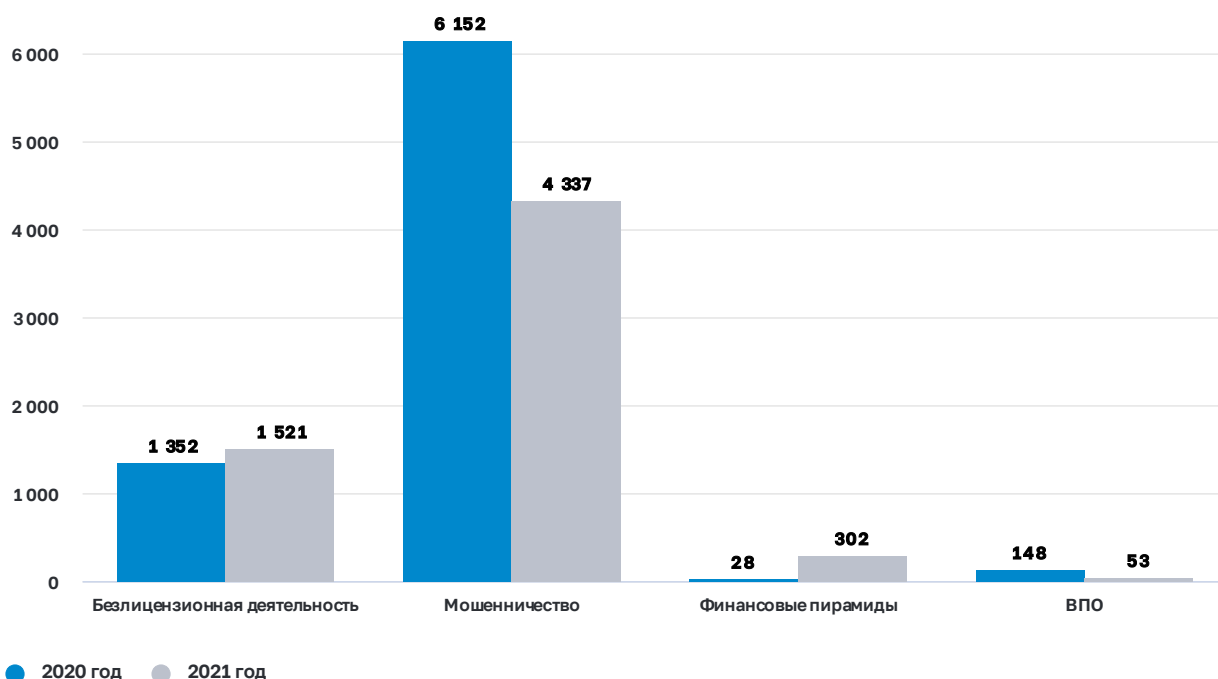
Сценарии звонков злоумышленников практически не изменились. По-прежнему использовались звонки от специалистов якобы «службы безопасности банка», «правоохранительных органов» и «Центрального банка», автоинформаторов и роботизированных помощников.

Совместно с Минцифры России и операторами связи Банк России продолжает работу по противодействию телефонному мошенничеству, совершаемому с использованием официальных номеров телефонов банков. Так, например, Банк России подготовил перечень телефонных номеров кредитных организаций, что позволило операторам связи заблокировать более 2 млн вызовов, которые пытались осуществить злоумышленники с использованием технологии подмены номера.

Атаки с использованием фишинговых сайтов

В 2021 году Банк России противодействовал интернет-ресурсам, с использованием которых злоумышленники осуществляли противоправную деятельность, а также рассылали вредоносное программное обеспечение (ВПО). В рамках этой деятельности Банк России взаимодействует с регистраторами доменных имен в зонах .ru, .РФ, а также в иных геодоменных зонах, направляя им информацию о выявленных ресурсах для их снятия с делегирования. В 2021 году Банк России направил в адрес регистраторов доменов информацию о 6213 ресурсах в сети Интернет, используемых злоумышленниками для совершения противоправных действий в финансовой сфере, что на 19% меньше, чем годом ранее (7680 ресурсов). Среднее время разделегирования доменов регистраторами составляет от 3 часов до нескольких дней.

Мошеннические интернет-ресурсы (ед.)



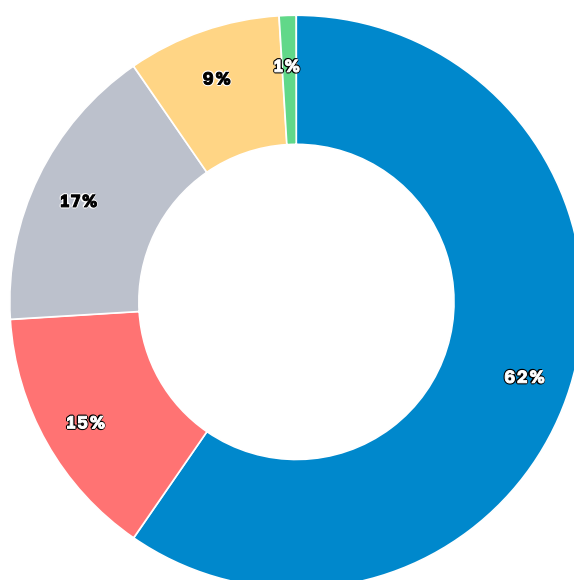
В 2020 году Банк России инициировал эксперимент по обмену информацией о мошеннических сайтах с Генеральной прокуратурой Российской Федерации для их блокировки. В 2021 году этот механизм был закреплен на законодательном уровне и Банк России получил право на внесудебную блокировку противоправных сайтов, по которому в 2021 году был ограничен доступ к 3 100 сайтам. Среднее время блокировки интернет-ресурсов, которые использовались для мошеннических действий на финансовом рынке и рекламы финансовых пирамид, сократилось с нескольких недель до нескольких суток.

Большая часть заблокированных сайтов (порядка 58%) использовалась для осуществления безлицензионной деятельности в сфере рынка ценных бумаг, а также рекламирования финансовых

пирамид. Злоумышленники активно похищали денежные средства клиентов под видом высокодоходных инвестиций в сельскохозяйственную, энергетическую отрасли, а также криптовалюту.

В 2021 году злоумышленники чаще всего маскировали фишинговые сайты под сайты действующих кредитно-финансовых организаций для получения персональных сведений пользователей или данных для входа в онлайн-банк, а также информацию по банковским картам. Кроме того, злоумышленники активно использовали сайты с информацией о возможности получения компенсационных выплат от государства или о возможности заработать денежные средства за прохождение опроса, теста и т.п. Актуальным направлением в 2021 году стали поддельные сайты известных маркетплейсов, магазинов по продаже электроники, бытовой техники, компьютеров и т.д.

Виды мошеннических сайтов



- Поддельные сайты финансовых организаций
- Опросы, социальные выплаты
- Поддельные сайты известных онлайн-магазинов
- Оплата билетов на любой вид транспорта
- Онлайн-кинотеатры

ⁱ В настоящем Обзоре приведены данные о количестве и объеме операций, совершенных без согласия клиентов, за 2021 год в сравнении с аналогичными показателями предыдущего года. Обзор составлен на основе сведений, предоставленных операторами по переводу денежных средств и операторами услуг платежной инфраструктуры в Банк России в рамках формы отчетности 0403203. Банком России на постоянной основе проводятся работы по улучшению качества данных по операциям без согласия клиентов, направляемых операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, в том числе в рамках надзорных мероприятий. По итогам указанной работы рядом организаций были направлены скорректированные данные по форме отчетности 0403203 ввиду различных причин (в т. ч. самостоятельно выявленных организациями ошибок в ранее представленных данных), что объясняет возникшую разницу в данных по операциям без согласия клиентов, представленных в настоящем Обзоре, и ранее публикуемых Банком России.

¹ Текущий показатель доли объема операций без согласия клиентов в общем объеме операций по переводу денежных средств учитывает операции, совершаемые с использованием не только платежных карт, но и иных электронных средств платежа.

² Расчет показателя доли операций без согласия клиентов, совершенных с использованием приемов и методов социальной инженерии, осуществляется на основе показателя количества операций без согласия клиентов.

Ответственное структурное подразделение: [Департамент информационной безопасности](#)

Последнее обновление страницы: 11.04.2022