

# ИБ и закон

Регулирование в области кредитного фрода становится строже. Однако, как показывают дискуссии на Уральском форуме по ИБ, ощущается недостаток в самых разных новых юридических актах, а также в поправках в существующие



Текст  
**ВАДИМ ФЕРЕНЕЦ,**  
ОБОЗРЕВАТЕЛЬ «Б.О.»

**В** преддверии Уральского форума «Кибербезопасность в финансах — 2024» зампред Банка России **Герман Зубарев** в интервью «Известиям» озвучил несколько тем, которые регулятор хотел бы там подробно обсудить.

В частности, летом 2023 года был принят закон по противодействию телефонным мошенникам, который ввел механизм возмещения банком похищенных денег, если его антифрод-системы некачественно сработали и допустили перевод. По новому закону им придется финансово отвечать за качество работы по этому направлению перед клиентами.

«Защитные автоматизированные системы зачастую становятся последним рубежом обороны на пути злоумышленников», — отметил зампред ЦБ. Однако этот рубеж не всегда срабатывает. Остается надеяться на юридическую защиту. Какие здесь сложились лучшие практики?

## Невероятно повезло с судьей

Немалый резонанс вызвала статья «Как IT-специалисты помогли выиграть суд у банка», опубликованная 13 января 2024 года на портале habr.ru. Ее автор, представитель юридической компании «Лазутченко и Паймухин» **Павел Лазутченко**, так описывает начало процесса: «Человек одним утром получил SMS о том, что он пропустил платеж по кредиту, который он не оформлял. В последующем выяснилось, что кредит оформлен онлайн в крупном банке в Санкт-Петербурге, при этом человек вообще ничего для этого

не делал, т.е. не называл никому коды из SMS, не вводил данные на каких-либо сайтах и никаким иным образом не способствовал заключению такого договора».

Чем осложнялось это дело? Какое-то время назад, будучи клиентом данного банка, этот человек брал здесь кредит. Соответственно банк знал этого клиента, имел его данные и действующее пользовательское соглашение. Это и подвело человека. Как выяснилось, жуликам до сих пор не установленным способом удалось войти в личный кабинет крупного сотового оператора, настроить переадресацию на свой номер и таким образом получить все SMS, которые отправлял банк своему клиенту.

Таким образом, банк, заключивший договор с жуликами, действующими от имени человека, имел все основания полагать, что договор с ним заключает полноценный заемщик, что делает подобный судебный процесс практически безнадежным.

Но не тут-то было. В суд было подано ходатайство об истребовании у банка документов — списка всех успешных и неуспешных авторизаций в личном кабинете. Это помогло установить, с какого IP-адреса была совершена операция по оформлению кредита.

Павел Лазутченко пишет: «В этом деле нам невероятно повезло с судьей. К сожалению, среднестатистический отечественный судья в районном суде никогда не будет слушать про какие-то IP-адреса и "интернет-гуглы". Но в этом споре нам действительно повезло! Суд удовлетворял все ходатайства о направлении запросов, действительно оказывал содействие в сборе доказательств, как того требует закон».

Не вдаваясь в дальнейшие следственные процедуры, юристам удалось добиться понимания у суда, что оформление кредита сопровождалось странными операциями, а также «красноречиво продемонстрировать ему подход банка к обеспечению безопасности». К чести банка, он все же заблокировал счета, правда, через несколько минут после того, как на них ничего не осталось.

В телеграм-канале «ИБ в Финсекторе», связанном с АРБ, произошла живая дискуссия по этому кейсу. Приведем несколько цитат из нее:

- «Уже тот факт, что конкретно в этом процессе суд удовлетворил ходатайства об истребовании у третьего лица сведений, составляющих тайну связи, — здорово»;
- «Чаще всего суды подобные доказательства клиентов отвергают, не рассматривая, и это плохо. Как здорово, что появляется практика нормального изучения доказательств»;
- «В свете отсутствия внятных требований к антифроду банков суды начинают заниматься откровенной отсебятиной. Не вижу в этом ничего хорошего».
- «Почему после смены реквизитов входа первый платеж не попал в антифрод? Наверное, потому, что антифрод "повесили" на ИБ, а не создали отдельное подразделение, специализирующееся на рискованных операциях».

### Полковник ФСБ на проводе

Приведем еще несколько показательных случаев, о которых на Первом канале ТВ в начале февраля 2024 года вышел сюжет в программе «Человек и Закон» и которые подробно разобрал адвокат правового центра «Человек и Закон» **Александр Спиричев**.

**Николая Иванова** из Москвы обманули стандартно. Звонок: «Полковник ФСБ на проводе, ваши счета под угрозой». Сначала мужчина перевел свои скопленные полмиллиона рублей на некие «секретные счета». Потом два экстренно взятых кредита — на 700 и 300 тыс. рублей. Наконец, пришла очередь квартиры.

Второй кейс связан с обманом и «перепривязкой» страницы жертвы на сайте «Госуслуги». Статистика говорит о том, что в последние месяцы идет массовый мошеннический обзвон в связи с необходимостью «пролонгации договора с сотовым оператором». И под эту «музыку» меняется пароль жертвы на сайте «Госуслуги».

Александр Спиричев рассказал: «Илья, по профессии дизайнер, современный молодой человек, про жуликов в курсе. Просто на автомате сообщил четыре цифры из СМС. А через десять минут ему позвонили с другого номера, представились “сотрудниками безопасности крупного банка”. Два часа ему морочили голову. Иначе он обратил бы внимание, что телефон постоянно пиликает. За это время взломали личный кабинет на сайте «Госуслуги» и личный кабинет банка, где у него хранились деньги, оформили кредит. Потерял много».

### Вести с Уральского форума

В ходе панельной дискуссии «Противодействие кибермошенничеству: ключевые вызовы и решения» с участием **Эльвиры Набиуллиной**, председателя Банка России, прошедшей в ходе Уральского форума «Кибербезопасность в финансах — 2024», была подтверждена острая проблема, связанная с кредитным мошенничеством: «Каждый четвертый рубль, который был похищен из банков кибермошенниками, является заемным».

Заместитель председателя правления Сбербанка **Станислав Кузнецов** отметил: «Все больше мошенничеств происходит с использованием кредитных средств. Сегодня это уже 30%

всех случаев, когда преступникам удается обмануть жертву и завладеть ее деньгами. В тех случаях, когда мы уверены, что клиент оформляет кредит под влиянием мошенников, мы вводим сами, без регулирования, период охлаждения. И 24 часов достаточно для того, чтобы жертва поняла, что ее обманывают. Эффективность периода охлаждения по кредитам близка к 100%». Сам же соответствующий закон о периоде охлаждения в двое суток должен вступить в силу только с июля 2024 года.

Суммируя сказанное участниками дискуссии, **Анатолий Аксаков**, председатель Комитета Госдумы по финансовому рынку, получил весомый список предложений:

- ускорить взаимодействие между банками, ведь нередко мошенники убеждают жертву оформить кредит в другом банке, который еще не в курсе того, для чего на самом деле оформляется кредит;
- создать единую платформу обмена рисковыми событиями для всех кредитных организаций в онлайн-режиме;
- ввести уголовную ответственность за дропкерство;
- законодательно перекрыть лазейки с сим-картами, когда необязательно верифицировать граждан, которые их получают, что является причиной появления сим-боксов;
- выработать единые подходы к статистике: они разнятся у банков, правоохранительных органов и регуляторов.

В свою очередь, Анатолий Аксаков, поддерживая мысль Эльвиры Набиуллиной, что в сфере борьбы с кредитным фродом пока еще нет системных барьеров, сообщил: «13 февраля на Комитете Госдумы поддержан законопроект о самозапрете онлайн-получения кредитов, и в течение нескольких дней он будет принят». **Б.О.**