Экономический факультет МГУ имени М.В. Ломоносова

Финансовая грамотность в вузах
ФЕДЕРАЛЬНЫЙ СЕТЕВОЙ МЕТОДИЧЕСКИЙ ЦЕНТР

ОЛИМПИАДА ПО ФИНАНСОВОЙ ГРАМОТНОСТИ

И.Б. Суркова, В.С. Трушина

Комплект аннотированных материалов для участников Олимпиады по финансовой грамотности 2018/2019

Москва, 2019

Оглавление

Введение

Уважаемые участники Олимпиады по финансовой грамотности (Всероссийский конкурс) 2018/2019!

Этот Аннотированный сборник материалов подготовлен, чтобы помочь вам в работе над аналитическими записками.

Первая часть Сборника посвящена преимущественно документам, определяющим условия и направления развития цифровой экономики в России. Здесь вы можете также найти ссылки на обзорные и аналитические материалы, как правило, выпущенные официальными органами.

Вторая часть Сборника содержит статьи, мнения, обзоры, другие материалы, посвященные проблеме, описанным в кейсах. Мы постарались собрать такие материалы, которые отражают разнообразие мнений по поднимаемым вопросам. И далеко не всегда составители сборника, организационный комитет и жюри мнения авторов этих материалов разделяют.

Возможно, ваши работы пополнят имеющееся многообразие точек зрения и идей. Но если вы присоединитесь к каким-то из тех, что представлены в Сборнике, это необходимо обосновать. Вы, безусловно, можете пользоваться и иными источниками информации (со ссылкой на них аналитической записке).

Желаем удачи!

I. Материалы, которые полезно изучить всем участникам Олимпиады

В разделе представлены ссылки на основные документы, определяющие направления развития цифровой экономики в России, а также ссылки на обзорные и аналитические материалы, посвященные отдельным аспектам применения цифровых технологий в финансовом секторе, в том числе, рискам для потребителей, возникающим в связи с применением этих технологий. Раздел содержит также ссылки на нормативные акты, проекты нормативных актов, содержащих положения, направленные на регулирование финансовых рынков и защиту прав потребителей финансовых услуг в условиях цифровой экономики.

1. Документы и материалы, определяющие направления и проблемы развития цифровой экономики в России, обеспечения прав потребителя и защиту от мошенничества

1.1. Программа "Цифровая экономика Российской Федерации" (Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. N 1632-р)

Программа определяет цели, задачи, направления и сроки реализации основных мер государственной политики России в период до 2024 года по созданию условий для развития цифровой экономики в рамках следующих основных направлений:

- нормативное регулирование;
- кадры и образование;
- формирование исследовательских компетенций и технических заделов;
- информационная инфраструктура;
- информационная безопасность.

Программа также обращает внимание на вызовы и угрозы, препятствующие развитию цифровой экономики России, к которым относит прежде всего:

- проблему обеспечения прав человека в цифровом мире, в том числе при идентификации (соотнесении человека с его цифровым образом);
- проблему сохранности цифровых данных пользователя, а также проблему обеспечения доверия граждан к цифровой среде;
- угрозы личности, бизнесу и государству, связанные с тенденциями к построению сложных иерархических информационно-телекоммуникационных систем, широко использующих виртуализацию, удаленные (облачные) хранилища данных, а также разнородные технологии связи и оконечные устройства;
- наращивание возможностей внешнего информационно-технического воздействия на информационную инфраструктуру;
- рост масштабов компьютерной преступности, в том числе международной;
- отставание от ведущих иностранных государств в развитии конкурентоспособных информационных технологий;

- зависимость социально-экономического развития от экспортной политики иностранных государств;
- недостаточную эффективность научных исследований, связанных с созданием перспективных информационных технологий, низкий уровень внедрения отечественных разработок, а также недостаточный уровень кадрового обеспечения в области информационной безопасности.

Программа содержит «дорожную карту», включающую описание целей, ключевых вех и задач Программы по основным направлениям, а также сроков их достижения. С текстом Программы можно ознакомиться на официальном сайте Правительства РФ по адресу http://government.ru/docs/28653/.

На этом же сайте http://government.ru/rugovclassifier/614/events/ содержится информация о ходе реализации национальной программы "Цифровая экономика Российской Федерации". Здесь, в частности, можно ознакомиться с утвержденными Планами мероприятий по основным направлениям Программы, а также с отчетами о ключевых событиях.

1.2. Стратегия государственной политики Российской Федерации в области защиты прав потребителей на период до 2030 года (Утверждена распоряжением Правительства Российской Федерации от 28 августа 2017 г. N 1837-р)

Стратегией, в частности, предусмотрено, что к числу приоритетных направлений государственной политики относится защита потребителей в сфере электронной торговли, а также названы некоторые проблемы потребителей в эпоху цифровой экономики.

С текстом Стратегии можно ознакомиться по ссылке http://static.government.ru/media/files/Bmcgd9cWb2UVctHrpF2nf9AMd4AA8dAf.pdf.

План мероприятий по реализации Стратегии содержится по адресу http://static.government.ru/media/files/b8LZ4vj5dxMOZjj8v43H6bXaqABaw5nG.pdf.

1.3. Основные направления развития финансовых технологий на период 2018-2020 годов, одобренные Банком России

Основные направления называют основные цели и задачи развития инновационных технологий на финансовом рынке РФ, в том числе:

- развитие цифровых технологий на финансовом рынке;
- переход на электронное взаимодействие между Банком России, участниками финансового рынка, физическими и юридическими лицами;
- обеспечение безопасности и устойчивости при применении финансовых технологий.

Основные направления включают описание предпосылок и трендов в сфере развития цифровых финансовых услуг в Российской Федерации, цели и ключевые направления деятельности Банка России в области финансовых технологий, а также описание соответствующих мероприятий.

Согласно Основным направлениям, предусмотренные мероприятия способствуют реализации программы "Цифровая экономика Российской Федерации", утвержденной Правительством Российской Федерации в июле 2017 года.

Текст Основных направлений можно открыть по ссылке http://www.cbr.ru/StaticHtml/File/36231/ON_FinTex_2017.pdf.

План мероприятий («дорожная карта») по реализации «Основных направлений развития финансовых технологий на период 2018-2020 годов» доступен по ссылке http://www.cbr.ru/StaticHtml/File/36231/roadmap_18_20.pdf.

Аналитические материалы, посвященные отдельным проблемам развития цифровых финансовых технологий, размещены Банком России по адресу: http://www.cbr.ru/fintech/analiticheskie-materialy/.

Обратите внимание, что Стратегия повышения финансовой доступности в Российской Федерации на период 2018–2020 годов (текст доступен по адресу http://www.cbr.ru/Content/Document/File/44104/str_30032018.pdf) рассматривает инновации в области цифровых финансовых технологий как обязательный элемент решения проблемы повышения доступности финансовых услуг для потребителей.

1.4. Концепция противодействия недобросовестным действиям на финансовом рынке, разработанная Банком России

Концепция охватывает отношения на страховом и микрофинансовом рынках, в сфере коллективных инвестиций и доверительного управления, а также на рынке ценных бумаг. Разработчиками сформулированы типичные схемы недобросовестного поведения на финансовом рынке, включающие кибермошенничество, «безлицензионную» деятельность, недобросовестные практики продаж финансовых услуг, формирование фиктивных активов и фальсификацию отчетности. Концепция содержит также перечень возможных мероприятий по борьбе с недобросовестными практиками и мошенничеством на финансовом рынке.

С текстом Концепции можно ознакомиться по ссылке http://www.cbr.ru/Content/Document/File/48603/concept_countering_unfair_actions.pdf.

2. Правовые основы цифровой экономики и защиты от мошенничества

В настоящее время права граждан при заключении и исполнении договоров с финансовыми организациями и иными поставщиками услуг, в том числе, при оказании услуг с использованием цифровых технологий, регулируются следующими правовыми актами:

2.1. Гражданский кодекс Российской Федерации N 51-ФЗ (с изменениями и дополнениями) от 30.11.1994

Первая часть Гражданского кодекса РФ устанавливает общие начала гражданского законодательства.

Раздел I. «Общие положения» содержит определения материальных и нематериальных благ, по поводу которых складываются регулируемые законодательством гражданские правоотношения, а также требования к порядку и форме заключения сделок.

ГК РФ допускает использование при совершении сделок электронной подписи либо иного аналога собственноручной подписи - в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон (статья 160), а также легализует заключение договора в письменной форме путем обмена электронными документами, передаваемыми по каналам связи, позволяющими достоверно установить, что документ исходит от стороны по договору (статья 434).

Раздел III. Общая часть обязательственного права (статьи 307 – 453) ГК РФ содержит общие положения об обязательствах и общие положения о договоре.

Вторая часть Гражданского кодекса РФ регулирует отдельные виды обязательств. Здесь определены существенные условия, права и обязанности сторон для отдельных видов гражданско-правовых договоров, в частности, договоров Возмездного оказания услуг (Глава 39), Заема и кредита (Глава 42), Банковского вклада (Глава 44), Банковского счета (Глава 45), Расчетов (Глава 46), Страхования (Глава 48).

Часто нормы этой части кодекса могут быть изменены по желанию сторон договора, на что в соответствующих статьях имеются специальные указания: например, используется формула «если иное не предусмотрено договором». Кроме того, многие нормы этой части могут быть уточнены (изменены) иными специальными законами – в этом случае соответствующая статья содержит указание «если иное не установлено законом».

Обратите внимание, что согласно Статье 847 "Порядок распоряжения денежными средствами, находящимися на счете", договором может быть предусмотрено удостоверение прав распоряжения денежными суммами, находящимися на счете, электронными средствами платежа и иными способами с использованием в них аналогов собственноручной подписи (пункт 2 статьи 160), кодов, паролей и других средств, подтверждающих, что распоряжение дано уполномоченным на это лицом.

2.2. Законодательство об обеспечении прав потребителей

2.2.1. Федеральный закон N 15-ФЗ "О введении в действие части второй Гражданского кодекса Российской Федерации" от 26.01.1996 (статья 9) устанавливает общее для всех видов гражданско-правовых договоров правило, согласно которому в случаях, когда одной из сторон в обязательстве является гражданин, использующий, приобретающий, заказывающий либо имеющий намерение приобрести или заказать товары (работы, услуги) для личных бытовых нужд, такой гражданин пользуется правами стороны в обязательстве в соответствии с ГК РФ, а также правами, предоставленными потребителю Законом о защите прав потребителей и изданными в соответствии с ним иными правовыми актами.

С текстом федерального закона можно ознакомиться по ссылке http://base.garant.ru/10105940/.

В отношении договоров, заключаемых финансовой организацией с гражданином, действует принцип «слабой стороны договора». Это означает, что гражданин признается экономически слабой и зависимой стороной договора, заключаемого с сильной стороной – финансовой организацией, и ему для гарантий соблюдения конституционного **принципа равенства сторон при осуществлении экономической деятельности** должны быть предоставлены определенные преимущества**.**

Этот аспект договорных отношений был отмечен в Постановлении Конституционного суда РФ от 23.02.1999 N 4-П по делу о проверке конституционности положения части второй статьи 29 Федерального закона от 3 февраля 1996 года "О банках и банковской деятельности" в связи с жалобами граждан О.Ю. Веселяшкиной, А.Ю. Веселяшкина и Н.П. Лазаренко. В частности, суд указал, что «граждане-вкладчики как сторона в договоре лишены возможности влиять на его содержание, что является ограничением свободы договора и как таковое требует соблюдения принципа соразмерности, в силу которой гражданин, как экономически слабая сторона в этих правоотношениях, нуждается в особой защите своих прав, что влечет необходимость в соответствующем правовом ограничении свободы договора и для другой стороны, т.е. для банков» (полный текст Постановления КС РФ доступен по ссылке http://www.garant.ru/products/ipo/prime/doc/12014558/).

Подробные разъяснения о свободе договора и ее пределах содержатся в **Постановлении Пленума Высшего Арбитражного Суда РФ от 14.03.2014 N 16 "О свободе договора и ее пределах" (текст доступен по ссылке http://www.arbitr.ru/as/pract/post_plenum/106573.html).**

2.2.2. Закон Российской Федерации N 2300-1 "О защите прав потребителей" от 07.02.1992

Закон направлен на обеспечение основных прав потребителя, а именно:

- права на безопасность товаров и услуг;
- права на получение информации, обеспечивающей возможность правильного выбора товаров (услуг);
- права на возмещение вреда, причиненного вследствие недостатков товара (работы, услуги), а также нарушения прав потребителя;
- права на судебную защиту.

Закон о защите прав потребителей применяется независимо от того, есть на него или нет ссылка в ГК РФ в случаях, если Закон о защите прав потребителей:

- конкретизирует и детализирует положения ГК РФ;
- регулирует отношения, не урегулированные ГК РФ;
- предусматривает иные правила, чем ГК РФ, когда ГК РФ допускает возможность их установления законами и иными правовыми актами.

Текст закона содержится по адресу http://base.garant.ru/5218829/.

При этом следует иметь в виду, что согласно **Постановлению Пленума Верховного Суда РФ от 28.06.2012 N 17 "О рассмотрении судами гражданских дел по спорам о защите прав потребителей"**, к отношениям, возникающим из договоров об оказании отдельных видов услуг с участием гражданина (например, договор страхования, договор банковского вклада и др.), Закон о защите прав потребителей, применяется в части, не урегулированной специальными законами.

Текст указанного Постановления ВС РФ имеется по ссылке http://www.garant.ru/products/ipo/prime/doc/70094860/.

С практикой применения законодательства о защите прав потребителей финансовых услуг можно ознакомиться в "Обзоре судебной практики по делам, связанным с защитой прав потребителей финансовых услуг" (утв. Президиумом Верховного Суда РФ 27.09.2017), опубликованном на официальном сайте Верховного суда http://www.vsrf.ru/documents/all/23996/.

2.3. Специальные законы, регулирующие отдельные виды деятельности по оказанию услуг гражданам и вопросы электронного взаимодействия сторон договора

2.3.1. Федеральный закон N 63-ФЗ "Об электронной подписи" от 6 апреля 2011 г. (с изменениями и дополнениями) (http://base.garant.ru/12184522/) регулирует правила использования электронной подписи регулируются. Закон также определяет виды электронной подписи – простую и усиленную, квалифицированную либо неквалифицированную. Сообщение с простой или усиленной неквалифицированной электронной подписью может быть приравнено к подписанному собственноручно бумажному документу, если стороны заранее об этом договорились, а также в некоторых указанных законом случаях.

2.3.2. Федеральный закон N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями) от 27.07.2006 (http://base.garant.ru/12148555/).

Закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий, в том числе, применении информационных технологий в целях идентификации граждан;
- обеспечении защиты информации.

2.3.3. Федеральный закон N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" (с изменениями и дополнениями) от 7 августа 2001 г. (http://base.garant.ru/12123862/).

Закон (статья 7) устанавливает порядок идентификации клиентов - физических лиц финансовыми организациями, в том числе, упрощенной идентификации и идентификации на основе биометрических данных.

2.3.4. Федеральный закон N 126-ФЗ "О связи" (с изменениями и дополнениями) от 07.07.2003 (http://base.garant.ru/186117/).

Закон устанавливает правовые основы деятельности в области связи на территории Российской Федерации, в том числе, обязанности операторов связи при предоставлении услуг гражданам, а также права пользователей услугами связи.

Законом, в частности, установлено, что услуги мобильной связи предоставляются только тем абонентам, достоверные сведения о которых предоставлены оператору связи (статья 44).

2.3.5. Федеральный закон N 161-ФЗ "О национальной платежной системе" (с изменениями и дополнениями) от 27 июня 2011 г. (http://base.garant.ru/12187279/)

Закон регулирует порядок оказания платежных услуг, в том числе, предоставления и использования электронных средств платежа (банковских карт, средств дистанционного банковского обслуживания, иных средств безналичных расчетов с использованием информационно-коммуникационных технологий).

Статья 9 Закона регулирует особенности заключения и исполнения договора об использовании электронного средства платежа, в том числе, правила информирования клиента о совершенной операции, правила приостановления оператором по переводу денежных средств использования клиентом электронного средства платежа в случаях выявления операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента, а также условия возмещения оператором клиенту суммы операции, совершенной без согласия клиента.

Признаки осуществления перевода денежных средств без согласия клиента утверждены приказом Банка России от 27 сентября 2018 года № ОД-2525 (http://www.cbr.ru/content/document/file/47786/priznaki_20180928.pdf).

Применение положений статьи 9 закона неоднократно комментировалось Банком России в форме ответов на вопросы по применению положений статьи, например, «Ответы на вопросы по применению статьи 9 Федерального закона «О национальной платежной системе» (http://www.cbr.ru/Content/Document/File/16195/faq_9.pdf), «Ответы на вопросы, связанные с применением отдельных норм Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (http://www.cbr.ru/Collection/Collection/File/238/faq_161.pdf).

2.3.6. Федеральный закон N 395-I "О банках и банковской деятельности" от 2 декабря 1990 г. (http://base.garant.ru/10105800/).

Закон устанавливает условия и правила осуществления организацией банковской деятельности, включая условия лицензирования кредитных организаций (выдачи и отзыва лицензии), общие правила осуществления отдельных банковских операций, обязанности банков по обеспечению устойчивости финансовой системы как основы защиты прав и интересов клиентов, общие правила взаимодействия банков с клиентами.

В декабре 2017 года в статью 30 Закона внесено дополнение, согласно которому договор между кредитной организацией и клиентом - физическим лицом, а также соглашение об электронном документообороте и иные документы, необходимые для обеспечения их взаимодействия после идентификации клиента - физического лица могут быть подписаны его простой электронной подписью, ключ которой получен при личной явке в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме. Указанные документы, подписанные простой электронной подписью, признаются электронными документами, равнозначными документам на бумажном носителе, подписанным собственноручной подписью данного физического лица.

2.3.7. Федеральный закон N 177-ФЗ "О страховании вкладов физических лиц в банках Российской Федерации" от 23.12.2003, регулирующий отношения по созданию и

функционированию системы страхования вкладов, выплатам возмещения по вкладам при наступлении страховых случаев.

Закон предусматривает выплату вкладчику суммы в размере 100 процентов суммы вкладов в банке, но не более 1 400 000 рублей, в соответствии с реестром обязательств банка перед вкладчиками. Выплата производится в течение трех рабочих дней со дня представления вкладчиком в Агентство по страхованию вкладов соответствующего заявления, удостоверения личности, доверенности представителя (если требуется по смыслу обращения).

Согласно Информации Банка России от 24 мая 2016 года "О документах, необходимых для выплаты возмещения по вкладам" (текст имеется по ссылке: http://www.cbr.ru/press/PR/?file=24052016_195302ik2016-05-24t19_51_36.htm), в случае отсутствия в банке документарного подтверждения обязательств перед вкладчиком вкладчику может быть предложено представить дополнительные документы, подтверждающие обоснованность его требований к банку:

а) договор банковского вклада (счета),

б) приходный ордер с отметками банка о внесении средств, или платежное поручение другого банка о перечислении денег на счет вкладчика, или иной документ, подтверждающий внесение денежных средств на счет банка и отвечающий требованиям, предусмотренным для таких документов законом, установленными в соответствии с ним банковскими правилами и применяемыми в банковской практике обычаями делового оборота, включая выписку с лицевого счета вкладчика, подписанную сотрудником банка и заверенную его печатью.

С текстом Федерального закона можно ознакомиться по ссылке: http://base.garant.ru/12133717/.

2.3.8. Федеральный закон N 151-ФЗ "О микрофинансовой деятельности и микрофинансовых организациях" (с изменениями и дополнениями) от 2 июля 2010 г. (http://base.garant.ru/12176839/) устанавливает права и обязанности заемщика и микрофинансовой организации, включая обязанность микрофинансовой организации по идентификации заемщика.

2.3.9. Федеральный закон N 353-ФЗ "О потребительском кредите (займе)" от 21.12.2013 (http://base.garant.ru/70544866/).

Закон регулирует особенности заключения, исполнения договора потребительского кредита (займа), в том числе, устанавливает обязанности кредитующей организации по предоставлению потребителю информации при заключении и исполнении договора, по расчету полной стоимости кредита, использованию электронного средства платежа при выдаче кредита, а также по предоставлению заемщику информации после заключения договора.

2.3.10. Федеральный закон N 40-ФЗ "Об обязательном страховании гражданской ответственности владельцев транспортных средств" от 25.04.2002 (http://base.garant.ru/184404/)

Законом определяются правовые, экономические и организационные основы обязательного страхования гражданской ответственности владельцев транспортных средств.

Закон устанавливает порядок заключения договора обязательного страхования на основании представленных страхователем электронных документов, составления договора обязательного страхования в виде электронного документа, правила электронного взаимодействия участников отношений по ОСАГО.

3. Обзорные и аналитические материалы

3.1. Множество информационных и аналитических материалов о реализации Программы «Цифровая экономика Российской Федерации» можно найти на сайте Аналитического **центра при Правительстве РФ**, выполняющего функции проектного офиса по реализации программы http://ac.gov.ru/projects/otherprojects/014091.html.

Здесь публикуются еженедельный дайджест «Новости цифровой экономики», а также информация и материалы обсуждений и дискуссий по вопросам определения основных терминов и понятий цифровой экономики, регламентов электронной цифровой подписи, использования персональных данных в сети Интернет, другим базовым вопросам.

3.2. Доклад Роспотребнадзора «О состоянии защиты прав потребителей в финансовой сфере в 2017 году»

Доклад подготовлен Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека при содействии ООО «Финансовые и бухгалтерские консультанты и содержит результаты анализа состояния и перспектив развития защиты прав потребителей в финансовой сфере в Российской Федерации по итогам 2017 года, включая результаты исследования нормативного правового регулирования защиты прав потребителей финансовых услуг, результаты анализа тенденций развития финансового рынка и рисков для потребителей финансовых услуг, обзор международного опыта в сфере защиты прав потребителей финансовых услуг, результаты статистического наблюдения и практики противодействия нарушению законодательных требований, обзор состояния информирования населения в сфере защиты прав потребителей финансовых услуг и повышения уровня финансовой грамотности, а также результаты деятельности крупнейших общественных объединений потребителей. Особое внимание в Докладе уделяется вопросам электронной коммерции.

Доклад опубликован на официальном сайте Роспотребнодзора и доступен по ссылке http://rospotrebnadzor.ru/deyatelnost/zpp/?ELEMENT_ID=10712.

На сайте Роспотребнадзора в разделе «Защита прав потребителей» имеются ссылки также и на выпуски таких докладов за предыдущие годы.

3.3. Информационно-просветительские ресурсы

3.3.1. Федеральный сетевой методический центр fingramota.econ.msu.ru

На сайте Федерального сетевого методического центра (ФСМЦ) в открытом доступе находятся аналитические и учебные материалы, комментарии экспертов по вопросам изменения законодательства и элементов институциональный среды, актуальные новости сферы личных финансов. Кроме того, пользователям сайта доступна база данных

финансовой статистики, разработан и внедрен инструментарий для анализа этой статистики.

Коллективом авторов создано электронное **Учебное пособие по финансовой грамотности для студентов** (**https://finuch.ru**), которое регулярно обновляется.

3.3.2. Финансовая культура fincult.info

Информационно-просветительский ресурс, созданный Центральным банком Российской Федерации с целью формирования финансовой культуры граждан. Сайт содержит материалы для потребителей финансовых услуг, преподавателей, методистов и волонтеров финансового просвещения.

3.3.3. Дружи с финансами vashifinancy.ru

Портал поддерживается Министерством финансов РФ совместно с Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека (Роспотребнадзор) в рамках реализации проекта Минфина РФ и Всемирного банка «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации».

3.3.4. Международная конфедерация общества потребителей (КонфОП) konfop.ru

На сайте публикуются результаты мониторинга рынков финансовых услуг, а также аналитические материалы о состоянии защиты прав потребителей для отдельных секторов финансового рынка.

II. Материалы для работы по отдельным темам

В Разделе II Сборника по каждой из предложенных тем содержатся информационные и аналитические материалы:

- публикации средств массовой информации о ситуациях, похожих на представленные в кейсах, или популярных комментариях, событиях, дополняющих такие ситуации;
- материалы судебной практики;
- статистические материалы, обзоры и комментарии экспертов;
- официальные документы, дающие представление о практических направлениях решения той или иной проблемы.

1. Кейс «Удаленная идентификация на основе биометрических данных»

Удаленная биометрическая идентификация физических лиц – клиентов финансовых организаций стала доступной летом 2018 года.

Сбора и использования биометрических данных граждан предусматривает следующие процедуры:

- сбор биометрических данных граждан (первичная идентификация) уполномоченным банком;
- регистрация гражданина в Единой системе идентификации и аутентификации (ЕСИА) (эта **система многим** знакома как обеспечивающая доступ к Порталу Госуслуг);
- размещение полученных биометрических данных в Единой биометрической системе.

Удаленная биометрическая идентификация позволит гражданину получить полноценное дистанционное банковское обслуживание – при обращении в новую финансовую организацию будет достаточно пройти авторизацию в ЕСИА и подтвердить свои биометрические данные.

В настоящее время биометрическая идентификация проводится на добровольной основе и только с согласия гражданина.

Применение удаленной биометрической идентификации клиентов в финансовой сфере регламентировано Федеральным законом №482-ФЗ от 31 декабря 2017 г. "О внесении изменений в отдельные законодательные акты Российской Федерации" (http://www.garant.ru/hotlaw/federal/1158557/). Изменения были внесены в Федеральные законы "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма", "Об информации, информационных технологиях и о защите информации", некоторые законы об отдельных видах деятельности на финансовом рынке.

Кроме правовых актов, указанных в Разделе 1, рекомендуется также ознакомиться с положениями Федерального закона "О персональных данных" от 27.07.2006 N 152-ФЗ, создающим, как в нем указано, правовую основу обращения с персональными данными физических лиц в целях реализации конституционных прав человека, в том числе права на

неприкосновенность частной жизни, личную и семейную тайну. Текст закона доступен по ссылке http://base.garant.ru/12148567/.

1.1. Официальные документы и комментарии

1.1.1. На официальном сайте Банка России в специальном разделе по адресу http://www.cbr.ru/fintech/remote_authentication/ размещены тексты нормативных документов, информацию и разъяснения о процедурах удаленной биометрической идентификации:

В разделе «Нормативные документы» доступны также тексты Постановлений и Распоряжений Правительства РФ, в том числе, регламентирующих форму согласия гражданина на обработку и хранение персональных биометрических данных гражданина; состав сведений, размещаемых в Единой биометрической системе.

1.1.2. Сведения о Единой биометрической системе содержатся на **официальном сайте ЕБС** https://bio.rt.ru/about/

1.1.3. Перечень угроз информационной безопасности определено в Указании Банка России от N2 4859-У/01/01/782-18 от 9 июля 2018 года, которые банки должны будут учитывать при сборе, использовании и передаче биометрических персональных данных своих клиентов (соответствующий пресс-релиз находится по ссылке http://www.cbr.ru/Press/event/?id=2005, а полный текст Указания – по ссылке http://www.cbr.ru/queries/unidbquery/file/50883?fileid=625).

1.2. Дискуссии: за и против

Биометрическая идентификация как в России, так и за рубежом является предметом активных дискуссий, и в Интернете легко найти множество статей и выступлений на эту тему. Ссылки на некоторые из них проводятся ниже:

- **Forbes – Добровольное принуждение: зачем банкам биометрия http://www.forbes.ru/tehnologii/368157-dobrovolnoe-prinuzhdenie-zachem-bankam-nuzhna-biometriya**

«Центробанк России представил карту банков, в которых любой гражданин может сдать свои биометрические данные. Предполагается, что это позволит совершать многие денежные операции удаленно и без банковских карт. Но кому в конечном счете пригодятся ваши биометрические данные?

Единая биометрическая система (ЕБС) начала работать спустя два года после заявлений Грефа о переходе на биометрию: с 1 июля 2018 года российские банки официально передают фотоизображения и голосовые профили граждан в централизованную базу. Восьмого октября 2018 года ЦБ РФ сделал еще один шаг к внедрению биометрии в банковском секторе и представил точки сбора по всей России. Отделения банков в 81 субъекте РФ принимают биометрические данные граждан.

Центробанк России представил карту банков, в которых любой гражданин может сдать свои биометрические данные: изображение лица и запись голоса. Для прохождения процедуры достаточно предъявить паспорт, СНИЛС и зарегистрироваться в Единой системе идентификации и аутентификации. ЦБ РФ сообщил, что биометрические данные

откроют гражданам удаленный доступ к банковским продуктам: вкладам, кредитам и переводам. Но дистанционное обслуживание на основе биометрии выгодно не только клиентам кредитных организаций. В чем интерес банков и государства?

От заявлений Германа Грефа к запуску ЕБС

Согласно исследованию международной консалтинговой компании Ernst & Young Global banking outlook 2018, до 60% опрошенных представителей международных банков планируют увеличить инвестирование в программное обеспечение на основе биометрии. Вместе с Россией в 2017 году в пятерку стран-лидеров по активности использования финтех-услуг вошла Великобритания.

Сбербанк России анонсировал внедрение биометрических технологий еще в мае 2016 года. Тогда Герман Греф объявил о постепенном отказе от пластиковых карт в пользу биометрии. Президент Сбербанка отметил, что решения на основе распознавания голоса и внешности доводят точность идентификации до 99,9%.

В июле 2016 года генеральный директор Национальной системы платежных карт (НСПК) Владимир Комлев поспорил с Грефом, заявив, что, несмотря ни на что, пластиковые карты еще много лет будут востребованы. Комлев оказался прав: пластиковые карты по-прежнему популярны у россиян. По данным ЦБ РФ по итогам 2017 года, операции по банковским картам выросли более чем на треть. Держатели карт, выпущенных российскими банками, совершили в прошлом году 24 млрд операций на общую сумму 63,4 трлн руб.

Тем временем на другом конце Европы британский телефонный и интернет-банк First Direct начал применять биометрию в обслуживании клиентов с марта 2016 года. Другой британский интернет-банк Atom Bank сообщил BBC, что использует технологию распознавания лица для регистрации клиентов. В августе 2016 года британский банковский конгломерат Barclays объявил о начале использования голосовых технологий для телефонного банкинга. Представитель банка заявил, что голос каждого клиента обладает набором более чем из 100 уникальных характеристик. Параметры зависят от физических особенностей горла и рта. По этой причине голос может служить идентификатором для доступа к банковским услугам, даже если пользователь забыл пароль.

В России, как и во всем мире, биометрия пока не заменила пластиковые карты. Однако уже в 2016 году Греф предрек тренд для всего банковского сектора, оценив срок внедрения биометрических технологий в 2-3 года. В июле 2017 года о своих планах по внедрению биометрии заявили ВТБ24, СМП Банк, Росбанк, Ситибанк, «Ак Барс» и Бинбанк.

Незадолго до официального запуска ЕБС в России Министерство внутренних дел Великобритании опубликовало проект создания единой биометрической базы данных. Новость вызвала резонанс и повлекла критику правозащитников, которые назвали проект «ночным кошмаром».

Биометрия для оптимизации

Биометрия не только распознает клиентов с вероятностью 99,9%, но и помогает автоматизировать взаимодействие с клиентами. Развитию автоматизации среди российских банков снова способствовал Сбербанк. В январе 2017 года зампред правления Сбербанка

Вадим Кулик заявил на Гайдаровском форуме, что робот-юрист позволит сократить 3000 юристов. Спустя неделю Герман Греф предположил, что численность персонала Сбербанка сократится в 2025 году в два раза в связи с цифровой трансформацией.

Роботы пока не привели к массовому исходу юристов из Сбербанка, но оптимизация банковских процессов отнюдь не пустой звук. Только за первые два квартала 2018 года Сбербанк сократил 11 000 сотрудников. Сбербанк не единственный банк, который ориентируется на автоматизацию как на способ экономии. В августе 2018 года Альфа-Банк объявил о планах по сокращению расходов на рутинные операционные процессы. Предположительно роботизация сэкономит для банка до 85 млн рублей ежегодно.

Голосовые технологии тоже способствуют автоматизации банковских процессов. Так, в августе 2017 года ВТБ24 сообщил об экономии 0,5 млрд рублей за два года с помощью IVR-системы автоматических голосовых сообщений: эта технология распознавания речи помогла клиентам банка находить ближайшие отделения. Тогда же пресс-служба финансовой организации сообщила о планах по переходу IVR на свободное распознавание речи.

Необходимость в экономии и периодическом сокращении персонала побуждает составлять планы по переходу на дистанционное банковское обслуживание на основе биометрии. Идентификация по голосу и изображению, которую запустили российские банки, в сочетании с системой IVR постепенно снизит присутствие сотрудников в банковских процессах. В первую очередь многочисленных сотрудников колл-центров.

База для «большого брата»

Анонс запуска ЕБС возник в контексте готовящегося ужесточения контроля над финансовыми операциями граждан. Яркое подтверждение тому – обсуждение запрета на снятие наличных с электронных кошельков и предоплаченных карт, которые не требуют идентификации пользователей и открытия банковского счета, в январе 2018 года.

Согласно данным ЦБ РФ, для удаленного доступа к банковским услугам с помощью биометрии недостаточно паспортных данных, СНИЛС, записи голоса и фотоизображения. Банк обязательно зарегистрирует гражданина в Единой системе идентификации и аутентификации (ЕСИА), а затем разместит полученные биометрические данные в ЕБС. Таким образом обогащение базы ЕБС означает обогащение базы ЕСИА. Предоставление гражданину удаленного доступа к банковским услугам, о котором заявляет ЦБ, невозможно без сопоставления данных ЕБС и ЕСИА.

ЦБ уже открестился от доступа третьих лиц к данным ЕБС. Так, в июле 2018 года ЦБ опроверг сообщения о том, что биометрические данные россиян из новой системы будут доступны коллекторам. Также российский регулятор публично дал понять банкам, что им придется обеспечить безопасность биометрии. В августе 2018 года ЦБ представил перечень угроз конфиденциальности информации ЕБС. К потенциальным угрозам ЦБ отнеснарушения: доступности (блокирование передачи), целостности (подмена, удаление) и конфиденциальности биометрических данных клиентов. Более того, безопасность биометрии потребует финансовых вливаний: так, главный операционный директор Альфа-банка Мария Шевченко оценила затраты на усиление криптографической защиты примерно в 7 млн рублей. И это довольно скромная оценка.

Несмотря на опровержение слухов Центробанком и борьбу с угрозами, запуск ЕБС означает появление единой и пополняемой базы биометрических данных граждан РФ. Согласно закону, который Госдума приняла в декабре 2017 года, оператор ЕБС будет предоставлять данные МВД и ФСБ в соответствии с процедурой, установленной правительством РФ. Таким образом, у планов Сбербанка и ЦБ РФ одинаковые причины. Предлог, который объединяет крупнейший банк и российского финансового регулятора, – удобство пользователей. Причина – сбор биометрических данных. Пока на добровольных условиях».

- **Банковское обозрение – https://bosfera.ru/bo/udalennaya-identifikaciya-chayaniya-i-realnost**

«Материалы онлайн-дискуссии представляют мнения профессиональных участников рынка о перспективах удаленной идентификации:

НУЖНА ЛИ БАНКАМ БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ? СКОЛЬКО КЛИЕНТОВ УЖЕ СДАЛИ БИОМЕТРИЧЕСКИЕ ДАННЫЕ?

Павел Чеботарев (Совкомбанк): Биометрическая идентификация нужна. Можно констатировать, что клиенты уже активно обращаются с вопросами по биометрической идентификации, но, к сожалению, пока 80–90% интересующихся – из числа наших же клиентов, желающих попробовать что-то новое. Сколько именно клиентов на сегодня сдали биометрию, сказать, к сожалению, не могу, пока это военная тайна.

Ксения Андреева (Райффайзенбанк): Стратегия у всех банков, по сути, одна – сделать жизнь клиента проще. В этом плане биометрия для нас – один из кусочков общего паззла, который позволит проще обслуживать клиентов, свободно работать в тех регионах, где нет точек физического присутствия Банка. Поэтому биометрия однозначно нужна, мы в нее очень верим. Что касается количества клиентов, сдавших биометрические данные, я не могу сказать, что есть значительный спрос, клиенты Банка не очень активны в этом отношении. Связано это отчасти с тем, что серьезной рекламной кампании по продвижению биометрии на рынке ни один банк не проводит. К тому же у нас на текущий момент работает только одно отделение в Москве, где мы обкатываем все процессы, смотрим, насколько это удобно для клиентов, насколько понятно. В целом, ситуация такова, что этот рынок только начинает формироваться, так что, думаю, спрос вырастет, но это произойдет позже.

Артем Харченко (Тинькофф Банк): Биометрия нужна, потому что человеку не всегда удобно ходить в отделение. Желание получить кредит здесь и сейчас, не выходя из дома, – это нормально, и это главное, зачем нужна биометрия.

Сандип Шарма (Альфа-Банк): Клиенту действительно важно получить свой продукт здесь и сейчас. Клиенты Альфа-Банка уже имеют возможность моментально получить кредит, дебетовую или кредитную карту. Биометрия и удаленная идентификация дают Банку возможность предоставить аналогичный сервис и новым клиентам. Количество сдавших биометрию на сегодня не измеряется тысячами, их достаточно мало. Это новаторы, которые хотят попробовать технологию и понять, как она работает.

Елена Медведева (Хоум Кредит банк): Правда жизни состоит в том, что сегодня использовать биометрию гражданам фактически негде. Но мы верим в биометрию, и абсолютно точно будем ее использовать. В целом, понятно, что это большой и сложный

проект, нужно время на раскачку. У нас только 10% офисов сейчас работает с биометрией, но до конца этого года мы планируем запустить все. Дальнейшее – где и как мы будем эту технологию использовать – зависит от нас. В перспективе хотелось бы, чтобы к биометрии подключались и другие сервисы – например, из сферы государственных услуг. Что касается конкретных данных, то в разных каналах привлечения количество клиентов, которые обращаются в Банк впервые, разнится от 50 до 70%.

Марина Фролова (Росбанк): Биометрия нужна, за ней будущее. Перед гражданами будут открываться все новые и новые возможности – как финансовые, так и нефинансовые – например, упрощение паспортного контроля при пересечении границы. Росбанк готов принимать и оказывать данный сервис гражданам в 61-м отделении, а до конца года подключим еще около 40, так что Банк выполнит все требования ЦБ. Если говорить о том, кто приходит в отделение сдавать биометрию, то пока это не те граждане, кому нужна некая банковская услуга в дальнейшем, а те, кому это просто интересно.

Андрей Шурыгин (Почта Банк): Привлечение клиентов через удаленный канал – это, как известно, бизнес, в котором для каждого клиента своя стоимость привлечения. Единая биометрическая система – это просто еще один канал такого привлечения, и мы очень надеемся, что эта история будет иметь большое развитие, а канал станет одним из самых мощных и быстрых. Мы ожидаем, что с ростом популярности биометрической идентификации, количества клиентов, сдавших биометрию, будет происходить перемещение клиентов из упрощенной идентификации в полноценную. Ведь это дает существенно большие возможности по использованию платежных средств, получению кредитов, размещению депозитов. Напомню, что Почта Банк одним из первых подключился к сбору биометрии – более чем в 120 отделениях по всей стране предоставляется эта услуга. С июля заработал интернет-банк с услугами удаленной идентификации, открытия счета, есть действующее мобильное приложение с удаленной идентификацией через ЕБС. Больших потоков пока там нет, можно говорить о тысячах клиентов, но о десятках тысяч говорить рано.

Александр Сулимов (Сбербанк): Лицевая биометрия, биометрия по венозному рисунку, голосовая идентификация для удаленных каналов, таких как контактный центр, – все это позволит реализовать три вещи: сокращение операционных расходов, эффективную борьбу с мошенничеством и повышение продаж, повышение клиентской удовлетворенности. Биометрическая идентификация, реализованная в контактном центре для розничных клиентов, удобна тем, что не нужно вспоминать кодовые слова, долго отвечать на вопросы сотрудников контактного центра, можно сразу получить консультацию.

ПОЧЕМУ НЕКОТОРЫЕ БАНКИ ТАК И НЕ ПРИСТУПИЛИ К СБОРУ БИОМЕТРИЧЕСКИХ ДАННЫХ И ДАЖЕ РЕКОМЕНДУЮТ АРБ ОБРАТИТЬСЯ К ЦБ С ПРЕДЛОЖЕНИЕМ ОТСРОЧКИ ТРЕБОВАНИЙ О НОРМАТИВЕ В 20% ОТДЕЛЕНИЙ ДО ЗАВЕРШЕНИЯ ИСПЫТАНИЙ СООТВЕТСТВУЮЩИХ ОБЛАЧНЫХ СЕРВИСОВ ПО ИДЕНТИФИКАЦИИ И БИОМЕТРИИ В КОМПАНИЯХ ЦФТ И РОСТЕЛЕКОМ?

Елена Ходюня (ЦФТ): Действительно, некоторые банки сегодня еще не принимают биометрические образцы, находятся как бы в подвешенном состоянии, ожидая, что Банк России даст отсрочку. Причин много – одни по каким-то причинам никак не могут зарегистрировать информационную систему в ЕБС и ЕСИА, у других ресурсов не хватает,

потому что очень много процессов, требующих автоматизации к концу года. Компания ЦФТ технически уже готова, в том числе и в части облачных технологий. Продукты ЦФТ, относящиеся к биометрии, – это модуль регистрации в ЕБС и ЕСИА, модуль идентификации и модуль подписи. Модуль регистрации позволяет собирать биометрические данные, модуль идентификации – это такой адаптер, позволяющий общаться с клиентом, с банковской системой, с сайтом банка и с сервисами ЕСИА и ЕБС. Оба модуля поставляются, естественно, с API, то есть дают возможность подключиться к любой информационной системе банка. Все решения могут быть размещены в облаке ЦФТ, то есть процессы могут быть отданы на аутсорсинг.

Дмитрий Корэ: Закон был подписан 31 декабря 2017 года, вступил в силу с середины текущего года, так что времени у банков на подготовку, на мой взгляд, было достаточно. Причина отставания, скорее всего, – в инертности мышления. Я бы хотел сказать о другом: помимо использования биометрии для удаленного привлечения клиентов эта технология с успехом может использоваться и в других банковских процессах – обслуживание клиента операционистом в отделении, в системах ДБО, при организации доступа к сейфовым ячейкам. Именно такой подход мы начали реализовывать в Россельхозбанке.

ЧТО БАНКАМ В СВЯЗИ С БИОМЕТРИЕЙ НУЖНО МЕНЯТЬ В ПРОДУКТОВОЙ ЛИНЕЙКЕ?

Артем Харченко (Тинькофф Банк): Биометрия – это новый способ подписать договор и идентифицировать клиента, не более того. Поэтому в продуктовой линейке не надо ничего менять, надо просто понять, в какие продукты нужно встраивать процесс альтернативной идентификации. На самом деле биометрия нужна клиенту для его дальнейшей жизни в обществе, а в банк он приходит в первую очередь за выгодными для него продуктами – вкладом, кредитом, карточкой.

Павел Чеботарев (Совкомбанк): Возможно, имеет смысл модифицировать линейку в контексте кредитования через удаленную идентификацию клиентов, задать новую градацию с небольшими лимитами, набрать статистику и посмотреть, как это будет работать, в том числе в плане фрода и антифрода. Если клиент перебрал кредитов, предусмотреть личную явку в отделение банка на очную идентификацию, в соответствии с требованиями ЦБ.

Андрей Шурыгин (Почта Банк): Модификация продуктовой линейки под нужды биометрической системы вряд ли необходима. Это действительно просто новый способ подписания договора, и, по моему мнению, специализированных продуктов здесь быть не должно.

Сандип Шарма (Альфа-Банк): Модификация продуктовой линейки специально под биометрическую идентификацию не нужна. Актуальный тренд – сокращение и упрощение продуктовой линейки, выделение из нее флагманских продуктов. Именно с этой точки зрения должна работать и удаленная идентификация. У банка по-прежнему должна быть простая и понятная линейка продуктов, и она не должна зависеть от способа подписания договора. Гораздо важнее работать над последующим сервисом, чтобы клиент мог качественно, быстро, удобно оформить новый продукт.

Александр Сулимов (Сбербанк): Необходимо подстраивать под биометрию существующие продукты, а не создавать под нее новые. Нужна полная синергия каналов

обслуживания и продуктовой линейки. За счет этого достигается и удовлетворенность клиента, и прибыль для банка.

Марина Фролова (Росбанк): Модификации линейки не требуется. Гражданам необходимы простые, понятные продукты. Биометрическая система – один из способов, который просто предоставляет более широкие возможности для экономичного получения услуг банка в любое время, независимо от режима работы офисов.

НУЖНО ЛИ АКТИВНО ПРОДВИГАТЬ БИОМЕТРИЮ СРЕДИ ГРАЖДАН?

Андрей Шурыгин (Почта Банк): Хотелось бы видеть большее участие государства в продвижении сервиса биометрии, потому что банки продвигают его со своей позиции, как финансовые организации, а у государства должны быть свои интересы. Со стороны государства, по всей видимости, нужно пропагандировать цифровое будущее, рассказывать о том, какие государственные сервисы планируется сделать для граждан с использованием биометрии. Вместе с теми банкам тоже нужно популяризировать сбор биометрических данных, вести разъяснительную работу. Необходимо акцентировать внимание граждан на том, что со временем помимо банковских появятся и другие сервисы, возможно, возникнет связка между налоговыми и банковскими услугами. Тогда биометрия будет широко востребована, люди сами пойдут ее сдавать.

Марина Фролова (Росбанк): Агрессивной рекламы не нужно, но повышать финансовую грамотность и пояснять смысл биометрии при обращении клиента в банк стоит. Ведь это открывает более широкие возможности гражданам, они смогут получить услуги и непосредственно в банке, и дома, причем в любое время.

Елена Медведева (Хоум Кредит банк): Частному банку активно вкладываться в рекламу сбора биометрии неэффективно и дорого. Даже если какие-то продукты уже можно получить удаленно, это еще не полный спектр, и понятно, что у клиента не так много выбора, где он может это использовать. Безусловно, хотелось бы сильной поддержки со стороны государства, потому что проект действительно большой, важный.

Сандип Шарма (Альфа-Банк): Участие государства в продвижении биометрии однозначно необходимо, иначе банки будут осуществлять это очень долго».

- **Bankir.ru – Пятое У, или Ужасы биометрии: почему вам опасно связываться с биометрической системой удаленной идентификации**
  https://bankir.ru/publikacii/20180508/pyatoe-u-ili-uzhasy-biometrii-pochemu-vam-opasno-svyazyvatsya-s-biometricheskoi-sistemoi-udalennoi-identifikatsii-10009496/

«В России скоро можно будет брать кредит, открывать счет, лишь показав себя камере смартфона (компьютера) и сказав несколько слов в его микрофон. Но в этих технологиях скрываются большие проблемы.

Те, кто продвигает новую технологию – а это (в порядке заинтересованности) Банк России, вендоры оборудования, технологий, «Ростелеком», Минкомсвязь и просто любители новых технологий, – используют понятие «четыре У» (универсальность, удаленность, уникальность, удобство). По-честному следовало бы говорить о «пяти У», добавив еще одну составляющую – увод денег.

Фигуры умолчания

Из существующих технологий создания биометрического профиля – считывание карты вен, радужки глаза, отпечатка пальца, сканирование лица, запись голоса и множество других – выбраны две: сканирование лица и запись голоса. Главная проблема всех без исключения технологий, связанных с биоидентификацией, проста: их можно обмануть. Для лица делается маска, голос синтезируют. Причем для обмана того же Face ID на iPhone не требуется делать полную копию лица, достаточно только копии областей вокруг глаз. А синтезатор голоса уже массово доступен.

Именно у этих двух выбранных технологий (сканирование лица и запись голоса) «идентификаторы» (лицо и голос) общедоступны. То есть вы постоянно даете возможность сделать копии своих идентификаторов. Камера на улице или в помещении, кто-то в магазине, в кафе могут записать ваши идентификаторы и сделать по ним свою копию. Особенно учитывая темпы развития компьютерной 3D-графики и 3D-принтеров.

Да, разработчики могут настроить систему удаленной идентификации на минимальную вероятность подделки предлагаемых «образцов» (то есть бороться с ошибкой первого рода). Но тогда вы часами будете снимать селфи и что-то говорить в телефон, поскольку значительно возрастет вероятность ошибки второго рода – непринятия ваших данных как настоящих.

У одного из крупнейших бюро кредитных историй в нашей стране биометрия используется для выявления загримированных мошенников или переклеенных фотографий. Система FPS. Биометрия делает это с вероятностью всего лишь около 80%, что гарантирует вычистку массы жуликов (умеренно низкая вероятность ошибки первого рода), но эта вероятность означает, что вас крайне редко (вероятность – 0,0000001) ошибочно могут принять за мошенника, поскольку последствия такой ошибки слишком велики (сдадут под белы руки в полицию). В этом примере решается специфическая задача. Но достаточно ли такой надежности (80%) для доступа к вашим счетам? Конечно, нет. Вам требуется более высокая вероятность, а значит, сложность взаимодействия с системой, при обеспечении безопасности, возрастает многократно.

По некоторым исследованиям, Face ID имеет показатель надежности лишь 98% при заявленных 99,9999%. И это при использовании специальной камеры, которой нет в массовых продуктах. Но не думаю, что вам понравится надежность в 98%. Это означает ложное срабатывание в двух случаях из 100. Разработчики удаленной идентификации, вероятно, надеются на совместное использование голоса и лица. Но голос дает слишком высокую вероятность ошибки и очень просто подделывается. Получается, что двухфакторная идентификация (перемножение вероятностей обмана с целью снизить итоговую вероятность) здесь практически не работает.

О чем они даже не задумывались

Сегодняшние системы биометрической идентификации работают совместно с традиционными «паролями» или обеспечивают доступ относительно небольшого числа людей к каким-то не столь важным функциям (разблокировке смартфона, например).

Складываются условия для комфортного, высокотехнологического, «чистого» – без личного участия – мошенничества

Но что же принципиально отличает удаленную идентификацию от биоидентификации в привычных нам приложениях? Ответ – удаленность. Гримированный

мошенник, приходящий в банк за кредитом с краденым паспортом, находится совсем в иных условиях, чем мошенник, работающий с «чужой личностью» по системе удаленной идентификации. «Мошенник на удаленке» находится в комфортных условиях, в любой стране мира, на любом континенте. Он знает о своей фактической безнаказанности: не пройти удаленную идентификацию – это значит «попробуем еще раз» с этим или другим профилем. То есть работаем дальше до очередного У – увода средств. А это не то же самое, что попасться с переклеенной фотографией или отклеившимися бровями в отделении банка. Складываются условия для комфортного, высокотехнологического, «чистого» – без личного участия – мошенничества.

А вот еще сюрприз

Преступник, прежде чем совершить преступление, может сколь угодно тщательно тестировать свою «модель идентифицируемого лица» на движках распознавания лица и голоса. Эти движки широкодоступны. Именно они лягут в основу строящейся системы удаленной идентификации. Если даже будет создана специальная версия движка для государственной системы биоидентификации, то можно будет или применить похожий движок (все современные системы схожи), или использовать версию для коммерческого применения.

По сути, «удаленка» бросает вызов хакерам по всему миру: взломай меня, если сможешь. Это напоминает классический хакатон. Только на кону стоит не надежность системы, а средства каждого гражданина (в качестве призового фонда). И куда гражданину обращаться, если его биопрофиль будет скопирован и применен?

Что же вам делать

Презентуемая в 2018 году система удаленной идентификации должна рассматриваться вами как еще одна «калитка» для мошенников к вашим деньгам. С простеньким замком. Сами решайте, надо ли вам это. Конечно, вы можете быть заинтересованы в простом доступе к кредитам или услугам и полагать, что терять вам нечего.

Часто люди, сообщающие номер мобильного телефона банку для получения СМС с балансом, не понимают, что им подключают еще и мобильный банк с доступом из него ко всем счетам

Но как насчет использования вашего биометрического профиля для открытия счетов с целью отмывания денег или использования кредитных средств без вашего ведома? В многочисленные черные списки сегодня легко попасть, но очень сложно из них выйти.

Если вы все-таки решитесь стать альфа-тестером для системы, то следует внимательно отнестись к новой реальности. Если к системе будет добавлен пароль к ЕСИА, вам следует изменить его на максимально защищенный. Очень часто люди, сообщающие номер мобильного телефона банку для получения СМС с балансом, не понимают, что им подключают еще и мобильный банк с доступом из него ко всем счетам. Или простенький пароль к «штрафам ГИБДД». А последствия одни и те же – потеря всех денег на всех счетах (а не только карточных).

Спецслужбам пригодится

Объективно разработчики систем удаленной идентификации могут рассчитывать только на массово используемые идентификаторы. Скажем, кроме биопрофиля, можно использовать электронный паспорт. Или информацию из кредитной истории, как в США. В Бельгии давно стали использовать электронный паспорт. Главная его ценность в том, что, докупив буквально за несколько евро считыватель информации, подключаемый к компьютеру по USB, вы приобретаете возможность удаленной идентификации физического лица. Да, это немодно и, главное, недорого. В нашей стране чиновники выбирают биоидентификацию.

Повторю вслед за представителем коммерческого банка, выступавшим на съезде АРБ в апреле этого года: «Сначала сделайте хотя бы нормально работающую проверку действительности паспорта и лишь затем увлекайтесь IT-проектами, требующими значительных затрат и не очевидно необходимыми». Да, может, вас это удивит, но технология не востребована финансовыми институтами, она «спущена сверху». Впрочем, биоидентификация может пригодиться коллекторам, чтобы опознавать своих должников, когда они прикидываются посторонними. Еще накопленная база биопрофилей пригодится спецслужбам. Пусть это и утешает любителей новых технологий».

- **Российская Газета – Свежая голова**
  https://rg.ru/2018/10/09/mihail-hazin-ia-nastorozhenno-otnoshus-k-edinoj-biometricheskoj-sisteme.html

«Лично я довольно настороженно отношусь к этой единой биометрической системе. Все, что где-то у кого-то хранится в электронном виде, может быть похищено злоумышленниками и использовано в любых незаконных целях. Да, нам обещают, что база данных будет хорошо защищена. Но мошенники разные бывают. В том числе и довольно грамотные, технически подкованные и способные взломать любую защиту. Это один момент.

Другой момент, который меня смущает, это надежность данной системы. Насколько стабильно и корректно она будет работать. Вот заболею я, к примеру, ларингитом, и система не сможет меня распознать. Скажет: «Нет, это не вы. У вас голос другой». Поскольку она еще совсем новая, то на первых порах неизбежны неполадки и ошибки в ее работе. Что тоже, кстати, может быть использовано разного рода злоумышленниками. Ну и в дальнейшем, что помешает кому-то записать мой голос на диктофон, идентифицироваться с его помощью в качестве клиента какого-нибудь банка и оформить на меня огромный кредит? У нас микрофинансовые организации по одной лишь копии паспорта деньги выдают. Даже не по оригиналу, а по копии. Что на руку мошенникам, берущим займы на других людей, которые до поры до времени ничего об этом не подозревают. Узнают лишь тогда, когда им начинают приходить письма с требованием исполнить долговые обязательства. Но доказать свою непричастность к этим кредитам потом оказывается нелегко. А копию паспорта заполучить, между прочим, несколько сложнее, чем образец голоса. В общем, пока я не готов воспользоваться данной услугой. А дальше видно будет.

Банкам-то понятно, что это выгодно. Они смогут сократить количество своих отделений и штат сотрудников. Соответственно, уменьшить расходы. Ну и привлечь новых клиентов. Из числа так называемых маломобильных групп населения и тех, кто живет в отдалении от крупных городов, и, следовательно, банковских отделений.

Закредитованных граждан у нас теперь может стать больше. Хотя их и так чуть ли не полстраны. С 2009 года у нас вдвое выросло число людей, имеющих непогашенные кредиты. Но это объяснимо. Материальное положение россиян ухудшилось. В то время как ставки по кредитам немного снизились. С одной стороны, я считаю, что нормальный человек в нашей стране кредитов брать не должен. Но с другой - понимаю ту же женщину, в одиночку воспитывающую троих детей, когда к 1 сентября ей нужно собрать их в школу. Всех. Откуда ей столько денег взять? Приходится брать в долг у банка. Бывают вынужденные кредиты. А бывают и такие, без которых вполне можно обойтись. На новую модель смартфона или иную дорогостоящую технику. Это уже блажь. Надо стараться жить по средствам. И с малых лет учить этому своих детей, чтобы в будущем у них возникало как можно меньше финансовых проблем».

- **Ведомости – Мы все разговариваем по телефону, и никто не боится, что его голос запишут**
  https://www.vedomosti.ru/newspaper/characters/2018/05/22/770389-mi-vse-razgovarivaem-po-telefonu

«Биометрия безопасна с точки зрения защиты персональных данных и не входит в конфликт с текущим укладом жизни – люди сами публикуют свои фотографии и видео в интернете, считает Центробанк. Но есть и сложности – нужно соблюсти баланс между высокими требованиями к безопасности и стоимостью оборудования

– Механизм удаленной идентификации должен заработать с 30 июня. Сколько человек зарегистрируется в системе за первые полгода ее работы и, например, к 2020 г.?

– За первые шесть месяцев регистрацию могут пройти сотни тысяч человек.

– Насколько будет востребована услуга удаленной идентификации, проводились ли такие исследования в России?

– В России это можно будет оценить, когда услуги начнут оказываться удаленно. По данным J’son & Partners Consulting, к концу 2020 г. 86% смартфонов на мировом рынке будут иметь встроенные биометрические сенсоры. Это логичный вектор развития: если есть возможность получать услуги с использованием биометрических данных, этим стоит пользоваться.

– У людей может быть ментальный барьер использования биометрии.

– В чем барьер? Мы активно пользуемся сервисами, которые подразумевают применение биометрии. Мы оставляем отпечаток пальца на своих смартфонах. Мы все разговариваем по телефону, и никто не боится, что его голос запишут. Люди сами публикуют свои фото и видео в интернете. При удаленной идентификации у человека не запрашивают ничего из того, чего бы он сам не публиковал ранее или не использовал при взаимодействиях с организациями и госорганами. В любом случае данные будут собираться только с согласия клиентов.

– На презентациях говорят, что система удаленной идентификации безопасна. Чем?

– Безопасность будет обеспечиваться за счет криптографической защиты информации и каналов передачи как биометрических данных, так и другой информации. А система хранения данных устроена так, что персональные данные человека не находятся в

той же системе, что и биометрические. Для первых есть ЕСИА, для вторых – ЕБС. Биометрические данные будут храниться в обезличенной форме.

– Сейчас разрабатывается приложение для смартфона с защищенным каналом связи, которое нужно будет использовать при получении услуг удаленно. В нем будет применяться российская криптография. Позволит ли Apple загружать такое приложение?

– Эти вопросы сейчас в работе.

– Сколько банкам удастся сэкономить с помощью удаленной идентификации?

– Это сложная многофакторная модель. Согласно расчетам самих банков, в среднем они тратят около 1000 руб. на идентификацию клиента в отделении или через курьера. Эта сумма включает расходы и на оплату труда операциониста, и на аренду или содержание офиса, бумагу и т. д. При удаленной идентификации банк будет тратить в 3–4 раза меньше, основные расходы придутся на получение информации о человеке от ЕБС (согласно проекту приказа Минкомсвязи стоимость запроса составит 200 руб. – «Ведомости»). Расходы банков на оборудование будут окупаться за счет вознаграждения от оператора системы за сбор данных.

– По закону использовать систему смогут только банки, являющиеся донорами биометрических данных. Есть банки без отделений, например «Тинькофф банк». Смогут ли они использовать систему? Смогут ли курьеры проводить идентификацию?

– При разработке требований к сбору биометрии мы учитывали и то, что на рынке работают банки с различными бизнес-моделями, и в целом тенденцию сокращения отделений банков. Поэтому первичную регистрацию можно будет пройти не только в отделении.

– Сколько банкам придется потратить на подключение к системе и на оборудование для сбора биометрии?

– Расходы будут зависеть от требований к оборудованию и условиям для сбора биометрии, согласованных со всеми сторонами. Это будет разумная цена для любого банка.

– Почему сложно согласовать эти требования?

– Это компромисс. С одной стороны, мы должны обеспечить высочайший уровень безопасности. Требования согласуются с несколькими ведомствами, в том числе ФСБ, Минкомсвязи и др. С другой стороны, нужно учитывать стоимость оборудования и она должна быть адекватной. Банки смогут сами выбирать марки и модели.

– В какой стадии сейчас работа над проектом?

– Проводится разработка и тестирование ЕБС с участием банков, тестируется клиентский опыт и взаимодействие информационных систем. Клиентский опыт очень важен – пользоваться системой должно быть легко.

Чтобы проект запустился с 30 июня, нужно сделать очень многое и в правовом плане, и в технологическом. Необходимо разработать 19 нормативных актов, из которых уже изданы два. Банкам нужно закупить оборудование, обучить сотрудников. Сроки очень сжатые».

1.3. Имеющийся опыт и перспективы

1.3.1. «Обзор международного рынка биометрических технологий и их применение в финансовом секторе» Банка России выпущен в январе 2018 г. Он содержит анализ и прогноз развития мирового рынка биометрических технологий, международный опыт использования биометрических технологий в различных отраслях экономики и в финансовом секторе, а также основные аспекты развития биометрической идентификации в России. Обзор доступен по адресу: http://www.cbr.ru/Content/Document/File/36012/rev_bio.pdf

1.3.2. Опрос портала Гарант.ру

В конце 2018 года порталом ГАРАНТ.РУ задал читателям вопрос: планируют ли они открывать счета и получать кредиты с использованием механизма удаленной идентификации на основе биометрических данных?

Результаты опроса опубликованы на портале по адресу: http://www.garant.ru/ia/research/1233950/.

1.3.3. Обзоры аналитических изданий о перспективах и истории развития биометрических технологий

- **РБК – Биометрия выходит на рынки http://www.rbcplus.ru/news/5be9cbd87a8aa936c1e304a0**

«В государственных и коммерческих базах данных копятся персональные биометрические данные пользователей. В ближайшие годы во множестве отраслей ожидается бум новых технологий идентификации личности.

По прогнозу ООН и Всемирного банка, к 2030 году у каждого жителя планеты будет официальный цифровой идентификатор, или ID. Уже сегодня программы национальных цифровых ID развивают в Италии, Бельгии, Норвегии, Дании, Турции, Японии и других странах Азии, а также Ближнего Востока и Латинской Америки.

Защиту цифровой «личности» обеспечивают технологии идентификации. По данным американской Acuity Market Intelligence, более половины стран – членов ООН выдают биометрические паспорта. По данным МВД РФ, за восемь месяцев этого года было выдано 2,4 млн биометрических загранпаспортов – на 43% больше, чем за аналогичный период 2017-го. К 2030 году в стране планируется переход на паспорта в виде пластиковых карт.

В 2018 году в России стартовало сразу несколько проектов по сбору персональных биометрических данных. Банк России и «Ростелеком» запустили Единую биометрическую систему (ЕБС), которая позволит гражданам, сдавшим образцы голоса и лица, получать банковские сервисы дистанционно. К концу 2019 года практически все банки должны обеспечить клиентам возможность сдать такие образцы в своих отделениях. Параллельно Ассоциация разработчиков систем искусственного интеллекта готовит проект создания национального оператора биомедицинских данных.

Формирование баз данных по группе наиболее распространенных заболеваний займет от трех до пяти лет, прогнозируют в Российской венчурной компании (РВК), при

поддержке которой была образована ассоциация «Национальная база медицинских знаний».

Главным драйвером развития биометрических технологий в мире являются госинициативы, направленные на обеспечение национальной безопасности, говорится в «Обзоре международного рынка биометрических технологий и их применения в финансовом секторе» (2018) ЦБ.

Биометрия уже применяется на выборах для идентификации избирателей и исключения мошенничества. Подобный опыт имеется в Бразилии и других странах Латинской Америки (в том числе в Мексике, Венесуэле, Боливии), а также в ряде стран Африки (например, в Конго, Кении, Нигерии и Камеруне). Варианты введения биометрической идентификации на избирательных участках рассматривают и в России.

Однако наблюдается переход от традиционного использования биометрии в системах госбезопасности к коммерческому и пользовательскому применению, отмечают авторы отчета ЦБ РФ. В ближайшие пять–семь лет рынок биометрических систем будет активно развиваться именно в коммерческом сегменте, прогнозирует специализированный ресурс FindBiometrics.com.

Идентификация в коммерческих целях

По оценкам международной компании J'Son & Partners, к 2022 году доля коммерческих кейсов использования биометрии глобально составит около 55%, из них более 30% придется на финансовый сектор.

По словам директора по цифровой идентичности компании «Ростелеком» Ивана Берова, широкое распространение в банках биометрия получает благодаря двум ключевым преимуществам – безопасности и удобству использования. Например, в рамках Единой биометрической системы клиентов будут распознавать по голосу при звонке в банк.

Уже сегодня финансовый сектор является третьим по величине рынком для биометрических систем: по данным ЦБ, его доля составляет около 15%; доля сегмента здравоохранения – 9%, ретейла – порядка 5%.

Ключевой биометрической функцией смартфона пока является распознавание отпечатков пальцев. Согласно оценкам тайваньской Digitimes Research, в 2017 году поставки устройств с датчиками отпечатков пальцев составили 64% объема мирового рынка смартфонов, а к 2020 году их проникновение превысит 75%. В скором времени получат распространение камеры, которые позволяют сканировать отпечатки пальцев бесконтактным способом, отмечают аналитики ЦБ.

Количество мобильных устройств с функциями биометрии с 2016 по 2022 год, по оценке британской Juniper Research, увеличится почти в пять раз и достигнет 760 млн единиц. По прогнозам J'son & Partners, мировой рынок мобильной биометрии будет расти со среднегодовыми темпами 34% и его объем к 2022 году достигнет $47 млрд.

Внедрение механизма удаленной идентификации на финансовом рынке России, отмечается в отчете ЦБ, будет способствовать цифровизации и других секторов экономики.

Рынки применения

В медицине биометрия используется для мониторинга, идентификации пациентов без ID (например, без паспорта), а также в рамках национальных программ идентификации носителей ВИЧ по отпечаткам пальцев (действует в Африке). Одна из самых крупных национальных баз ДНК (более 5 млн профилей) уже сформирована в Великобритании.

В ретейле с помощью биометрических технологий оплачивают покупки, осуществляют мониторинг поведения покупателей в целях предотвращения краж и повышения их лояльности благодаря релевантным предложениям и промоакциям.

По подсчетам Juniper Research, объем транзакций в мобильных устройствах с помощью биометрических технологий к 2023 году глобально превысит $2 трлн – это в 17 раз больше прогнозного показателя 2018 года ($124 млрд). Быстрее всего будет расти количество удаленных транзакций (свыше 48 млрд к 2023 году, или 57% от общего числа). Для сравнения: по итогам этого года доля транзакций с биометрическим подтверждением прогнозируется на уровне 28%.

В офисах биометрия вытесняет привычные магнитные карты, PIN-коды и пароли для идентификации сотрудников в системах безопасности, а также используется для учета рабочего времени и контроля дисциплины труда. В парламенте Аргентины, например, по результатам перехода на биометрию с начала 2018 года было выявлено до 700 сотрудников, периодически прогуливающих работу. Фитнес-клубы уже заменяют клубные карты системами распознавания клиентов по лицу.

Американская Tractica прогнозирует, что мировой рынок биометрии в целом будет расти до 2025 года на 22,9% ежегодно и составит более $15 млрд. К этому времени каждый третий новый автомобиль будет оснащен биометрией, прогнозируют исследователи компании Frost & Sullivan, что обеспечит повышение уровня безопасности на дорогах.

Технологии будут помогать с навигацией и управлением транспортными средствами. Другие подключенные устройства (интернет вещей, IoT) также будут использовать биометрические решения, ожидают в агентстве ResearchAndMarkets. В «умных» домах уже работает голосовое управление освещением и температурой. Потребительскую электронику (смартфоны, планшеты, фитнес-браслеты, «умные» часы и другие носимые устройства) будут все активнее оснащать сенсорами отпечатков пальцев, и объем только этого сегмента вырастет почти до $10 млрд к 2024 году.

В России, по прогнозам компании ЦРТ, рынок биометрической идентификации вырастет до $325 млн к 2019 году; в перспективе получат распространение такие надежные идентификаторы личности, как 3D-модель лица, радужная оболочка глаза и рисунок вен.

Консолидация данных

Пока каждая организация собирает собственную базу биометрических данных для решения локальных задач, говорит Иван Беров. Однако и в России, и в мире, по его словам, наблюдается тенденция к их консолидации: преимуществом такого подхода в первую очередь являются простота реализации конечных кейсов использования и безопасность хранения данных. Хранение биометрии в локальных базах повышает риск кражи цифровых идентификаторов, и гарантировать безопасность данных в десятках организаций, куда граждане соглашаются предоставить свои данные, сложно.

По данным «Ростелекома», сейчас с ЕБС взаимодействуют более ста банков, а создать цифровой образ можно более чем в 120 городах по всей России.

Уже при текущем объеме данных важно создавать однозначные связи между данными из разных источников, говорит генеральный директор VisionLabs Александр Ханин. Это, по его словам, позволит актуализировать существующую информацию и получать новые данные с большим количеством связей.

Крупнейшая в мире система полноохватной идентификации (AADHAAR) уже реализована в Индии – на начало 2018 года в ней были зарегистрированы 1,19 млрд человек, или 99% населения страны старше 18 лет. В системе хранятся фотография, отпечатки всех десяти пальцев, сканы радужной оболочки обоих глаз и стандартные персональные данные (ФИО, дата и место рождения, пол, адрес проживания, номер телефона, адрес электронной почты). Все эти данные привязаны к 12-значному идентификационному номеру, который используется при работе с различными государственными и частными сервисами.

E-Gates в Европу

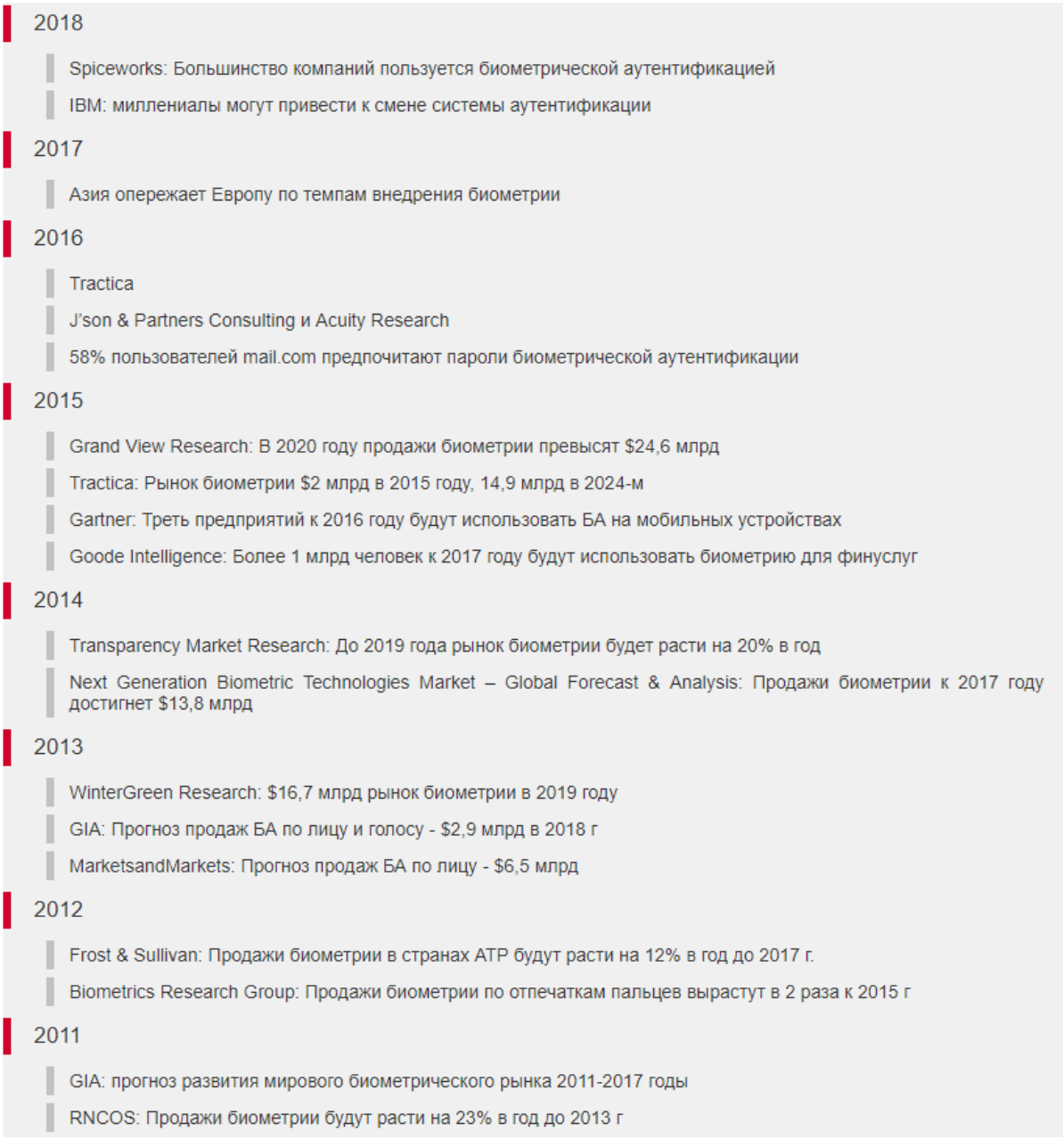
Евросоюз вводит электронный контроль (на основе отпечатков пальцев и по лицу) за пересечением границ стран-участниц. Речь идет почти о 1,8 тыс. пунктах, а также международных воздушных и морских портах. На Европу, по оценкам агентства Acuity, приходится около 36% всех установленных в мире биометрических систем e-Gates (еще около 40% – на страны Азии). К 2020 году их количество в мире вырастет до 6 тыс.

Кроме того, в странах ЕС реализуется пилотная программа EU's Smart Borders Initiative, предписывающая гражданам из других регионов идентификацию по лицу, радужной оболочке глаза и отпечаткам пальцев одновременно. В программе участвуют шесть аэропортов: Arlanda (Швеция), Charles de Gaulle (Франция), Frankfurt (Германия), Lisbon (Португалия), Madrid (Испания) и Schiphol (Нидерланды)».

- **Интересную хронологию применения биометрических технологий на мировом рынке выпустило аналитическое издание «Тэдвайзер» – Биометрическая идентификация (мировой рынок).**

  Полную версию хронологии можно посмотреть по ссылке: **http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%B8%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F_(%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%80%D1%8B%D0%BD%D0%BE%D0%BA)**

  Краткая версии хронологии выглядит следующим образом:



1.3.4. Публикации об оценке перспектив внедрения механизмов удаленной биометрической идентификации в России.

Различные экспертные источники по-разному оценивают перспективы технологии:

- **Ведомости – Банки начали погоню за биометрическими данными клиентов https://www.vedomosti.ru/finance/articles/2018/12/27/790574-banki-nachali-pogonyu**

> «Узнал из рекламы в банкомате Сбербанка, что скоро меня смогут «обслужить по лицу», – пошутил в Facebook один из клиентов банка, намекая на двусмысленность словосочетания «обслужить по лицу».
>
> В этом году Сбербанк пообещал, что в его офисах, банкоматах и мобильном приложении появится распознавание по лицу, а при звонке в колл-центр система сможет узнавать клиентов по голосу. В перспективе эти технологии помогут ускорить

обслуживание и повысить безопасность операций благодаря дополнительному фактору, позволяющему подтвердить личность.

Крупнейшие банки, в том числе российские, уже используют биометрические технологии в обслуживании: например, так они распознают клиентов при звонке в колл-центр или визите в сейфовое хранилище, ведут базу берущих заведомо невозвратные кредиты мошенников, собирая фото заемщиков. Кроме того, Россия – мировой лидер по платежам с помощью смартфонов, ряд которых также используют биометрические технологии (оплата подтверждается с помощью отпечатка пальца).

Не все технологии одинаково полезны

350 человек зарегистрировались в системе, позволяющей оплачивать покупки с помощью отпечатка пальца на кассе, в ходе пилотного проекта Сбербанка и «Азбуки вкуса», по данным J'Son & Partners. Представитель Сбербанка это не прокомментировал.

В этом году Сбербанк форсировал сбор биометрии: по словам его президента Германа Грефа, к декабрю банк собрал «миллионы образцов» биометрических данных клиентов, речь идет о слепках голосов и изображениях лиц. Собрать столько образцов Сбербанк смог в том числе за счет агрессивных продаж. Его сотрудники говорили клиентам, что с января, если биометрических данных нет в системе, обслуживание клиентов будет начинаться с их сдачи, правда, пресс-служба заявляла, что с Нового года ничего не изменится.

Почему Греф хочет превратить Сбербанк в IT-компанию

По количеству собранных биометрических данных клиентов Сбербанк на несколько порядков обгоняет запущенную с конца июня государственную Единую биометрическую систему (ЕБС), единожды сдав в которую изображение лица и слепок голоса человек может в любом банке получать кредиты, открывать счета и делать переводы без визита в отделение. Антиотмывочный закон требует от банков идентифицировать всех новых клиентов, и теперь сделать это они могут не только при личном присутствии клиента, но и с помощью ЕБС.

Собирать биометрию для ЕБС обязаны все банки, но пока это делают немногие, а оказывают услуги с ее помощью – лишь единицы. В итоге к октябрю в ЕБС сдали данные лишь 2000 человек, актуальную цифру оператор системы – «Ростелеком» не раскрывает.

Кому нужна единая биометрическая система

Причина того, что люди не торопятся сдавать данные в ЕБС – ограниченное количество услуг, которые можно получить с ее помощью, признают сами банкиры. Депутаты уже пытаются это исправить: они внесли законопроект, согласно которому с помощью ЕБС можно получать большинство банковских услуг. Кроме того, сдать данные пока можно лишь в небольшом числе отделений, да и Сбербанк, обладающий крупнейшей сетью, подключился к ЕБС только в конце декабря.

Самое большое свершение этого года – вступление в силу закона об удаленной идентификации и начало наполнения ЕБС, говорит президент СРО НАПКА Эльман Мехтиев. По его словам, можно говорить об укреплении тренда на все большее использование новых технологий в финансовых услугах. Но важно, чтобы применение

биометрии расширили на большее количество услуг: ее ведь можно использовать для идентификации повсеместно, подчеркивает он.

Особенностью российского финтеха является значительное присутствие Банка России: инициативы регулятора стали самыми обсуждаемыми (в их числе и создание ЕБС), говорит председатель наблюдательного совета ICONIC Елена Титова, в остальном активность на этом рынке низкая. При этом важны не только технологии как таковые, но и правовая база под них: например, биометрия без возможности удаленного открытия счетов была бы не так интересна, подчеркивает Титова».

- **News.ru – Банки раскошелятся на биометрию**
  https://news.ru/den-gi/banki-biometriya-informaciya/

«Подключение банка с одним отделением к системе будет стоить 3–4 млн рублей

В России определились с перечнем «базовых элементов», который будет необходим кредитным организациям для сбора биометрической информации и передачи её в Единую биометрическую систему. Предполагается, что подключение финансовой организации с одним отделением обойдётся в 3–4 млн рублей, каждый последующий офис будет стоить 130 тысяч рублей.

При этом банкам не удастся избежать расходов, так как к концу следующего года сбор биометрии будет обеспечен во всех кредитных организациях. Но те банки, которые практически не работают с населением, будут освобождены от груза обязанностей.

Соответствующие вопросы поднимались на закрытом совещании в «Ростелекоме», пишет «Коммерсант». Оно было посвящено исполнению финучреждениями требований информационной безопасности при сборе биометрии. Согласно данным источников издания, в нём участвовали представители ЦБ, ФСБ, а также топ-20 отечественных банков. В ходе совещания особое место было уделено вопросам безопасности: у банка в обязательном порядке должен быть установлен антивирус и настроена система обнаружения угроз.

По итогам заседания и был утверждён список «базовых элементов» для подключения к системе биометрии, благодаря которому можно рассчитать все затраты на данные процедуры. Так, необходимая настройка оборудования и аттестация системы ЕБС – всё это потребует от банков около 1,2 млн рублей. Также после присоединения к системе кредитным организациям придётся тратить по 800 тысяч рублей на годовое обслуживание.

Напомним, что к 1 января подключиться к системе должны 20% отделений банков, к 1 июля – 60%, а к концу следующего года – 100%.

Сейчас в России действует менее 500 банков, а собирают биометрическую информацию только 50. По состоянию на 2 августа в системе находились данные всего 1200 человек. Это крайне мало для окупаемости проекта. Безусловно, сначала банкам предстоит потратиться, и финансирование для внедрения оборудования ложится на плечи самой кредитной организации. В этой связи могут подорожать годовое обслуживание пластиковых карт, использование мобильного банка, комиссии за переводы и т.д.

Важно понимать, что некоторая часть кредитных организаций сконцентрирована на обслуживании корпоративных клиентов. В этой связи поток клиентов, желающих сдать биометрию, будет там, скорее всего, минимальным.

Биометрия как часть жизни

Как отметила News.ru руководитель аналитического департамента компании «ФинИст» Екатерина Туманова, сбор биометрических данных – это новый элемент в жизни россиян. На самом деле эта процедура упрощает жизнь многим, так как теперь не обязательно ходить в банк, всё можно делать по телефону или планшету. Достаточно сходить один раз и оставить свои данные.

«Подобная система используется уже в Индии – она позволяет пользоваться фактически любыми услугами: получения талонов на еду, социальных субсидий и топлива для кухни до расчётного счёта в банке, кредитов, страховки, пенсии, операций с недвижимостью и т.д.», – отметила Туманова.

По её словам, чем быстрее будет пополняться база ЕБС, тем быстрее банки почувствуют выгоду. И такая система выгодна финансовым учреждениям – банк сможет сократить штат сотрудников, в будущем сократить отделения, при этом эффективность станет лишь расти, потому что всё постепенно будет переходить в дистанционное обслуживание.

«Но готово ли население? Скорее всего, молодежь, маломобильные граждане, занятые бизнесмены будут более активны в этом вопросе. Вторая часть первое время будет наблюдателем и примкнет к первым, когда убедится, что эта система работает на благо», – сказала она.

Но всё новое воспринимается сначала критично, а потом уже мы привыкаем к новым удобствам.

Борьба за каждого клиента

Со своей стороны эксперт Международного финансового центра Гайдар Гасанов заявил, что стимулом для сбора биометрических данных клиентов банка послужили несколько причин. По сути, главная из них – безопасность. Стоит отметить, что современные банковские системы безопасности довольно неплохо справлялись со своими обязанностями, но в силу высокого роста информационных технологий необходимо не оставаться на месте и совершенствовать каждую отдельно взятую структуру банковского сектора, в том числе и сферу безопасности.

«В настоящее время среди банков зашкаливает конкуренция за платёжеспособного клиента. Особенно если речь идёт о тех клиентах, которые имеют депозиты в банках. Первостепенная задача банка – обеспечить надёжность и сохранность средств вкладчиков», – сообщил Гасанов.

Поэтому решение о переходе на сбор биометрических данных основано как на вопросе безопасности, так и удобства идентификации клиента, а также на сохранении времени при открытии депозитов или выдаче кредитов.

Сейчас если и пугает цифра расходов на переход к сбору биометрических данных и биомониторингу, то в любом случае именно наличие биометрической информации намного сократит расходы, связанные с обслуживанием клиентов.

«Это может отразиться на сокращении расходов при обслуживании клиентов. Сотрудникам физически не обязательно будет присутствовать при оформлении депозитов

или выдачи кредитов. Всё будет происходить дистанционно, при этом во много раз сократится и время обслуживания», – считает эксперт.

В настоящее время каждый банк индивидуально создаёт подобную систему биометрии, но когда будет сформирована единая биометрическая база, то это будет некий стандарт для всех банков, что, безусловно, сократит время на поиск вариантов забора биометрических данных клиентов. Так или иначе банкам придётся нести расходы на сбор биометрии за счёт как депозитных, так и кредитных портфелей.

И за чей счёт?

В свою очередь главный аналитик «Телетрейд Групп» Олег Богданов заявил, что если банки понимают, что конечные расходы лягут на их клиентов, то они готовы идти на любые траты.

«Поэтому говорить о том, что расходы на биометрию сильно повлияют на финансовое положение наших банков, я бы не стал. Да, есть проблемы у банков, которые обслуживают в основном корпоративных клиентов, однако и в этом случае или их исключат из списка обязательного подключения, или они переложат груз расходов на своих клиентов через увеличение различного рода комиссий и ставок», – сказал Богданов.

Конечно, банки вполне могли бы обойтись и без сбора биометрической информации, но есть закон, который в целях безопасности устанавливает необходимость и регламент данной процедуры. Возможно, будут внесены поправки, чтобы не пострадали небольшие корпоративные банки, так как в нынешнем варианте закона не предусмотрено исключений.

Необходимость сбора биометрических данных диктуют потребности национальной финансовой безопасности, поэтому сомневаться можно только в деталях этого закона, в нынешних сложных условиях такой закон, конечно же, необходим».

- **Коммерсант – в Биометрия для больших**
  https://www.kommersant.ru/doc/3766881

«Ряд банков могут освободить от сбора и передачи данных

Не исключено, что от сбора биометрических данных граждан для последующего дистанционного представления доступа к банковским услугам могут освободить небольшие банки. Многие из них активно не работают с физлицами и не имеют специального оборудования для проверки подлинности паспортов. В таких банках предлагают сбор биометрических данных доверить только крупным игрокам, оставив мелким возможность дистанционной верификации клиентов. ЦБ пообещал проработать этот вопрос.

Вопрос об освобождении небольших банков от сбора биометрических данных и передачи их в единую систему (ЕБС) был поднят на международном форуме «Вся банковская автоматизация». В частности, руководитель службы информационной безопасности Златкомбанка Александр Виноградов отметил, что у небольших игроков есть единственный способ проверить подлинность представленного паспорта – это просветить на ультрафиолете. «Ту же вклейку определить невозможно», – добавил он. Банками было оглашено предложение допустить к сбору биометрии лишь тех игроков на рынке, которые обладают необходимым оборудованием для проверки подлинности документов. По словам участников дискуссии, это крупные кредитные организации и розничные игроки, активно

работающие с физлицами. Небольшие же банки будут заниматься исключительно верификацией клиентов (то есть подтверждением их личности) при обращении к ним дистанционно за услугами. Заместитель руководителя управления департамента информационной безопасности ЦБ Ольга Краева заверила рынок, что данное предложение вполне логично и будет проработано.

Эксперты считают, что, если предложение будет реализовано, это повысит защищенность граждан от противоправных действий мошенников. «Не стоит забывать, что сейчас много липовых кредитов выдается именно по поддельным документам, – рассуждает управляющий партнер «Ренессанс-Lex» Георгий Хурошвили. – По липовой биометрии за короткий срок можно набрать множество кредитов в различных банках, поэтому крайне важно максимально защищать клиента от возможности попадания чужих биометрических данных от его имени в ЕБС». Небольшие игроки не скрывают свой интерес к подобному подходу, поскольку он позволит сократить им расходы на закупку оборудования для сбора биометрии. Сейчас минимальная стоимость комплекта – от 4 млн руб. на закупку всего оборудования, из которых 1,5 млн руб. приходится на HSM-модуль (позволяет дистанционно передавать данные в зашифрованном виде).

Впрочем, есть и другой вариант решения проблемы – аутсорсинг, когда съем биометрических данных и/или верификацию за небольшого игрока будет делать его более крупный партнер. На недавней встрече с банковским сообществом «Ростелеком» заявлял, что вопрос передачи сбора и верификации биометрии на аутсорсинг «технологически решается легко, но не юридически и регуляторно». В частности, к такому подходу крайне настороженно относится ЦБ. «Предоставление банкам возможности делегировать обязанность по сбору биометрических персональных данных иным организациям влечет риски подмены персональных данных и снижения достоверности идентификации граждан, – сообщили в пресс-службе ЦБ. – В настоящий момент данный вопрос не рассматривается». В «Ростелекоме» на запрос “Ъ” сообщили, что также не рассматривают возможность реализации сбора биометрических данных методом аутсорсинга. «Ростелеком» будет совершенствовать систему и готов учитывать пожелания банков, однако изменения в системе, связанные с риском для персональных данных пользователей, неприемлемы, отметили там.

Впрочем, реализовать компромиссный вариант и освободить небольшие банки от непосильной обязанности проводить сбор и передачу биометрических данных быстро не удастся. Потребуются поправки к законодательству, поскольку сейчас банки обязаны по требованию клиента снять биометрию и передать его данные в ЕБС. Тем временем, согласно действующим нормам, уже к концу года все банки должны обеспечить сбор данных и передачу в ЕБС в 20% своих отделений, а к концу 2019 года – в 100%. Помимо готовности рассмотреть предложение со стороны ЦБ потребуются согласие заинтересованных ведомств, подготовка законопроекта и рассмотрение его Госдумой.»

- **Коммерсант – Биометрии не хватает мобильности**
  https://www.kommersant.ru/doc/3753577

«Криптографическая защита не помещается в смартфоны

Банки уже три месяца собирают биометрические данные граждан. Но, как выяснил “Ъ”, предоставление на их основе услуг с помощью мобильных устройств до сих пор

невозможно. Проблема во многом заключается в действующих требованиях к уровню криптографической защиты. В ряде случаев их выполнить настолько трудно, что приходится искать компромисс в ущерб информбезопасности.

Как стало известно “Ъ”, серьезной проблемой предоставления услуг гражданам на основании ранее сданных биометрических данных стала ограниченная возможность использования мобильных устройств для верификации клиента. В первую очередь – из-за необходимости применения средств криптографической защиты.

Сбор биометрических данных населения стартовал в банках в начале июля (см. “Ъ” от 2 июля). Сданные биометрические данные (образ лица и голос) направляются в единую биометрическую систему. В дальнейшем для получения банковской услуги человеку достаточно пройти авторизацию в единой системе идентификации и аутентификации и подтвердить свои данные с помощью смартфона, планшета, ноутбука или компьютера с камерой и микрофоном.

Мобильное приложение, которое будет устанавливать клиент на своих гаджетах для верификации и получения дистанционных банковских услуг, сейчас разрабатывает «Ростелеком». Его представление предварительно планируется на середину октября. Однако с размещением этого приложения в PlayMarket и AppStore возникли проблемы.

Приложение защищено криптографией, то есть Apple и Google должны дать согласие на внедрение черного ящика в свои магазины приложений, – поясняет “Ъ” эксперт, близкий к "Ростелекому». – И если от Google такое согласие получено, то с Apple переговоры все еще ведутся».

Факт переговоров подтвердил “Ъ” и заместитель главы департамента информационной безопасности ЦБ Артем Сычев.

В Apple не ответили на запрос “Ъ”. В «Ростелекоме» от комментариев отказались. Но если переговоры с Apple не увенчаются успехом, то счастливые обладатели айфонов не смогут пройти верификацию через мобильные устройства и будут вынуждены при обращении в банки делать это только с компьютера или планшета через веб-приложение.

Впрочем, остаются и другие сложности с использованием биометрии. По словам консультанта по интернет-безопасности компании Cisco Алексея Лукацкого, срок сертификации средств шифрования в ФСБ обычно длиннее времени жизни пользовательского и банковского ПО. Такое несовпадение по времени приводит либо к использованию несертифицированной, но самой последней версии ПО, либо к работе с устаревшим, но обладающим сертификатом программным обеспечением. В данном случае обновление версий операционных систем потребует оперативной пересертификации программы в ФСБ. Артем Сычев заверил “Ъ”, что проблемы не возникнет. Однако сейчас сертификация занимает не менее года.

Проблемы порождают и разночтения в нормативных документах. По словам Алексея Лукацкого, есть установленные нормативными документами требования ФСБ для средств криптографической защиты (СКЗИ), которые непросто выполнить на платформах Macbook, iOS и т. п. «В соответствии с действующими документами ФСБ при наличии доступа нарушителя к исходным кодам операционной системы (а такая возможность есть для Linux и Android), на которой будет запускаться биометрическое ПО, сертификация возможно только по классу КА, что невозможно выполнить», – отмечает господин

Лукацкий. Однако Банк России в указании 4859-У, определяя перечень угроз при работе с биометрическими данными, счел достаточным более низкий уровень защищенности – КС1. Еще один нормативный документ ФСБ, по словам экспертов, требует поэкземплярного учета СКЗИ. «Однако при скачивании приложения для верификации с мобильных телефонов обеспечить поэкземплярный учет невозможно, как и невозможно обеспечить СКЗИ класса выше КС1 на мобильном устройстве», – отметил директор по управлению рисками Почта-банка Святослав Емельянов.

По словам правозащитников, подобный подход явно ущемляет права банковских клиентов. «Когда человек сдает биометрию, он рассчитывает с ее помощью оперативно получать доступ к банковским услугам, – рассуждает руководитель проекта ОНФ "За права заемщиков" Виктор Климов. – И о том, что приложение не будет функционировать на его телефоне, он должен быть проинформирован в момент сдачи биометрии, а не постфактум». Так же как он должен быть заранее и подробно проинформирован о рисках, в том числе – получения доступа злоумышленников к его биометрическим данным, резюмировал он».

2. Кейс «Заем поневоле»

Для работы по этому кейсу полезно обратиться к положениям статей Уголовного кодекса РФ, в том числе, определяющих составы отдельных видов преступлений:

- Статья 159. Мошенничество;
- Статья 159.1. Мошенничество в сфере кредитования;
- Статья 327. Подделка, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков.

"Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (с изм. и доп., вступ. в силу с 08.01.2019) доступен по ссылке http://base.garant.ru/5761709/.

2.1. О возможных схемах кредитного мошенничества, консультации и советы по безопасности

Тема кредитного мошенничества с оформлением кредита по чужим документам или данным очень популярна в Интернете – вы самостоятельно сможете найти описание различных схем мошенничества и множество советов, как себя от таких мошенников обезопасить. Ниже представлены некоторые из таких материалов (за реалистичность сценариев, впрочем, отвечают опубликовавшие их авторы):

- **KreditorPro – Можно ли по чужим паспортным данным взять кредит? http://kreditorpro.ru/mozhno-li-po-pasportnym-dannym-vzyat-kredit/**

«По мере развития популярности онлайн-кредитования участились случаи мошенничества. Клиентов волнует вопрос, как защитить свои персональные данные от рук хакеров и не оказаться в кредитной яме.

Часто можно встретить вопрос на форумах и в сообществах социальных сетей – «Может ли другой человек взять кредит по моим паспортным данным?». Из-за боязни клиенты часто отказываются пересылать документы кому бы то ни было посредством Интернета, и также боятся вводить свои данные на сайтах.

Оправданны ли страхи заемщиков? И может ли мошенник в действительности оформить кредит, имея в наличии только паспортные данные клиента? Об этом мы и поговорим в данной статье.

Хакеры и их уловки

Чаще всего воровством персональных данных занимаются хакеры. На деле это могут быть как молодые ребята, еще не достигшие совершеннолетия, так и взрослые и вполне уважаемые люди, тщательно скрывающие свои «дурные наклонности» от окружающих.

В Сети можно найти множество форумов, где общаются так называемые «манимейкеры», и ужаснуться множеству схем «честного отъема денег у населения». В данной статье вы найдете информацию о том, как мошенники берут кредиты.

На таких форумах нередко встречаются темы, наподобие перечисленных ниже:

- Есть сканы паспортов и вторых документов, как оформить на них кредит. О том, можно ли получить деньги по сканам или ксерокопиям паспорта, читайте здесь;
- Продам пакеты бумаг на дропов;

- Где можно оформить займ или кредит онлайн с получением на электронный кошелек. Подробнее об оформлении займа на Вебмани, вы узнаете по данной ссылке;
- Куплю симки с оформлением по скану паспорта;
- Куплю карты, оформленные на дропов, с целью вывода средств;
- И т.д.

Мотивация проста – мошенников отнюдь не привлекает честный труд, а раздобыть сканы при необходимости можно в той же социальной сети «В Контакте», где есть определенные ошибки. В частности, все бумаги, загружавшиеся пользователем в раздел «Документы», доступны для поиска остальным пользователям данной социальной сети.

И среди этих файлов каждый день появляются сотни сканкопий, которые и используют в своих махинациях последователи Остапа Бендера.

Итак, что же нужно мошеннику при оформлении кредита по чужим данным?

1. Паспортные данные и сканкопии.
2. Вторые документы – загранпаспорта, права, ИНН и СНИЛС (данные или сканкопии).
3. Данные о месте работы – не обязательно, часто мошенники ставят данные компании, взятые из того же Интернета.
4. Информация о кредитной истории заемщика – для адекватных мошенников это обязательный пункт. Перед подачей заявок в банки они проверяют информацию о клиенте, чтобы не тратить свое время понапрасну. Те люди, которые имеют плохую КИ, их не интересуют, так как таким заявителям банки отказывают. Больше информации о том, что собой представляет такое досье и о его важности, вы получите здесь.
5. Симкарта, оформленная на паспортные данные клиента.
6. Карта для вывода средств, и их последующего снятия.

При наличии скана паспорта и соответствующих связей получить все необходимое не составляет труда. Но тут перед мошенником появляется новая трудность.

Банки не выдают кредиты без личного присутствия заемщика. Подделать паспорт, переклеив фотографию на нужную, могут далеко не все хакеры, предпочитающие «не светиться» в офисах.

Онлайн-кредиты в МФО

До недавнего времени сферой деятельности мошенников являлись онлайн-микрозаймы, которые представляли собой широкое поле для деятельности за счет различных способов перечисления денежных средств. В настоящее же время и среди таких компаний практически не осталось лазеек для «манимейкеров».

МФО совершенствуют собственные системы защиты, и, как правило, требуют именные банковские карты с целью верификации заемщика. А с получением именно таких карт на данные «дропов» у мошенников обычно проблемы, так как их оформление также требует личного присутствия.

Исключение составляли разве что банковские карточки платежных систем Яндекс.Деньги, КИВИ и Вэбмани. Но микрокредитные организации не позволяют пройти верификацию с их помощью. И это указано в правилах компании на сайте.

Перечисление средств в большинстве МФО при первом обращении клиента производится на банковскую карту. Остальные способы получения средств (электронные деньги и наличные переводы) доступны только после успешного погашения первого займа.

В связи с этим, возможности мошенничества и оформления кредитов по паспортным данным без присутствия самого заемщика упали практически до нуля. И единственное, что теперь могут сделать хакеры – это продать пакетами собранные персональные документы клиентов для иных целей.

Как правило, их покупают те, кто занимается обналичиванием ворованных с чужих счетов денег, недобросовестные агенты НПФ и иные третьи лица.

Как защитить свои персональные данные от кражи?

Заемщикам, волнующимся за сохранность своих документов, стоит соблюдать ряд нехитрых правил, чтобы уберечь свои персональные данные от кражи:

- Не использовать для пересылки сканкопий бумаг социальные сети;
- Не вводить персональные данные на неизвестных сайтах;
- Регулярно проверять свою кредитную историю на предмет появления новых счетов. По данной ссылке рассматриваем порядок действий при обращении в НБКИ;
- Не хранить личные документы в облачных хранилищах;
- Не пересылать, по возможности, бумаги посредством электронной почты или же ставить водяные знаки на сканкопиях, чтобы защитить их;
- Не отправлять свои фотографии с паспортом в руках посторонним лицам или неизвестным компаниям;
- Регулярно менять пароли от почтовых ящиков и аккаунтов социальных сетей на сложные.
- Если в какой-либо организации вам необходимо показать свой документ или серию идентификационного номера, то вы можете следить за всеми действиями, которые производит сотрудник во время проставления штампов, ксерокопии документов, оформления займов, совершения обменных операций и в других ситуациях.

Очень часто вам нужно предоставить копии своих документов при получении какой-либо услуги, например – оформлении кредита, получении новой сим-карты, обращения в различные государственные структуры и т.д. При этом многие волнуются – не будут ли использованы мои личные данные без моего ведома?

На самом деле, здесь защита достаточно проста: непосредственно на самой ксерокопии, в свободном месте, прямо от руки ручкой напишите: «Копия изготовлена для получения кредита\оформления сим-карты» и т.д. Вы имеете на это полное право, если будут отказываться принимать – зовите директора.

Соблюдение этих правил позволит защитить персональные данные от кражи и избежать проблем в будущем. Если вы столкнулись с ситуацией, когда кто-то оформил кредит по вашим паспортным данным, немедленно обращайтесь с заявлением о мошенничестве в полицию.

Что делать, если кто-то взял кредит по вашему паспорту и вам звонят из банка

Первое, что необходимо сделать – успокоиться и не накручивать себя по поводу возможных предстоящих разбирательств. Существует вероятность, что произошла какая-то ошибка. Это выяснится уже на этапе телефонных переговоров. В финансовом учреждении должны все тщательно перепроверить.

Однако, если кредитор все же требует от вас оплаты по кредиту, который вы не оформляли, попробуйте обратиться в службу безопасности банка с письменным заявлением с подробным описанием ситуации. Кроме того, письмо можно отправить по почте.

Если вы утеряли паспорт, то об этом следует незамедлительно сообщить в милицию. Вам необходимо получить копии бумаг по займу, чтобы разобраться в сути требований кредитора и возбудить дело по факту мошенничества.

Вы вправе получить копии КД и дополнения к нему, а также копию квитанции, которая подтверждает факт получения вами денежных средств. Также нужно обязательно получить документы, на которых имеется ваша подпись. Кредитная организация должна произвести внутрибанковскую проверку и отменить свои претензии.

Что делать, если банк не слушает вас

За чужой долг платить, конечно же, не нужно. Сделайте кредитору подробный запрос по кредитному договору и идите с ним в суд. Если он отказывается, тянет время и запутывает всю сложившуюся ситуацию, не забывайте, что в течение этого времени растет процент.

Поэтому обращаться в органы следует как можно быстрее. По мнению специалистов, нужно воспользоваться графологической экспертизой, которая поможет доказать вашу непричастность к оформленной ссуде.

Помните о том, что единственный способ взять кредит на чужого человека, который не предполагает сговора с клиентом и мошенничества со стороны банковского работника – очень качественная переклейка фотографии в паспорте. В остальных случаях имеет место участие конкретного сотрудника финансовой организации.

Для защиты своих клиентов от преступных действий некоторые банки выработали определенные методики, среди которых наиболее эффективной является фотографирование заемщика. Это и поможет впоследствии идентифицировать, был ли во время оформления заема конкретный человек или нет».

- **PR-CREDIT.RU – Как мошенники оформляют микрозаймы?**
  https://pr-credit.ru/kak-moshenniki-oformlyayut-mikrozajmy/

«В современном мире оформить микрозайм не составляет особого труда. Для этого требуется минимальный список документов и немного свободного времени. Привлекательны такие банковские услуги для частных клиентов, а также для мошенников. Случаев, когда злоумышленник регистрирует заём на имя другого субъекта довольно много. О таких ситуациях сообщают в СМИ, да и банковские структуры свидетельствуют об этом. В статье предлагаем рассмотреть, как можно получить микрозайм по чужому паспорту, зная, как работает эта система, можно обезопасить свои деньги.

Для привлечения новых клиентов финансовые организации упростили форму получения кредита. Если в банке нет чётких правил и требований при оформлении

микрозайма, то этот факт создаёт предпосылку для злоумышленников. Которые готовы воспользоваться возможностью и незаконно оформить кредит, по данным чужого паспорта.

Одним из распространённых способов, является сговор с сотрудником микрофинансовой организации (МФО). В таких случаях мошенник делает вид, что он является владельцем паспорта, по видеонаблюдению этот обман выглядит вполне правдоподобно. Приходит клиент, предъявляет паспорт, ведёт себя адекватно, подписывает документы и получает деньги. При этом все фигуранты мошенничества (сотрудник банка, кассир и т. д.) вознаграждаются определённой суммой из выданного кредита. Нужно подметить, что обычно, такие махинации раскрываются при расследовании дела. И мошенничество можно будет доказать в суде. При этом все участники несут уголовную ответственность.

Как взять микрозайм на чужой паспорт онлайн?

С появлением доступного интернета микрозайм можно оформить, на чужой паспорт, онлайн. Оформляя онлайн-кредит, не требуются оригинал паспорта и другие документы. Достаточно знать данные, записанные в паспорте и некоторые сведения о человеке. Список информации для заполнения онлайн-формы при получении микрокредита:

1. Фамилия, имя, отчество.
2. Дата, месяц, год рождения.
3. Серия, номер, кем и когда выдан паспорт.
4. Прописка.
5. Номер телефона заёмщика, а также поручителей или родственников.
6. Фактическое место работы, кем работает сумма ежемесячной зарплаты.
7. Ксерокопия паспорта.

Мошенники заняты вопросом, как обмануть микрозайм. Но здравомыслящему человеку необходимо серьёзно подходить к вопросу об обеспечении сохранности своих документов и информации. Придерживаясь рекомендациям, приведённым в этой статье, Вы обезопасите себя от негативных последствий.

Обычно аферисты подбирают банк, где оформляется срочный микрозайм с упрощенными условиями подачи документов. И при помощи банковских интернет-услуг, оформляют заявку на получение микрокредита. Виртуальная заявка рассматривается в режиме онлайн также и проверка документов осуществляется дистанционным способом. Одобрение и выдача кредита происходит также по интернету.

Получение средств происходит через «Киви-кошелёк» либо на банковскую карту. Первый вариант получения денег самый распространенный. Зная информацию и паспортные данные, мошеннику не составляет труда оформить «Киви-кошелёк» и микрозайм на чужой паспорт. А также некоторые микрокредитные компании готовы перечислить средства на электронный кошелёк «Яндекс-деньги», возможны и другие варианты.

«Как взять микрозайм на чужой паспорт» – это довольно частый запрос в поисковых системах интернета

Изучив популярные интернет-сайты, которые предоставляют кредиты по интернету. Задали поисковый запрос: «как оформить микрозайм на чужой паспорт». Далее, предлагаем Вам таблицу с актуальной информацией.

Название кредитной компании	Способы перечисления денег	Максимальная сумма кредита	Срок кредита
«У Петровича»	Киви-кошелёк, Яндекс-деньги, Банковская карта, Контакт система.	50 тыс. рублей	От 2 месяцев до 1 года
«iZaimo»	Киви-кошелёк, Яндекс-деньги, Банковская карта, Контакт переводы.	50 тыс. рублей	От 2 месяцев до 1 года
«Quickzaim»	Киви-кошелёк, Яндекс-деньги, банковская карта.	50 тыс. рублей	От 2 месяцев до 10
«Kredito 24»	Банковская карта.	30 тыс. рублей	От 7 дней до 30 дней
«Вкармане»	Банковская карта.	20 тыс. рублей	От 5 дней до 30 дней

Удивляет тот факт, что таких кредитных компаний больше сотни, и каждая предлагает оформление, и одобрение микрозайма за несколько минут, в большем случае за час. При этом оформление полностью происходит дистанционно, некоторые сайты вообще не требуют документы, нужна только информация. А другие готовы оформить кредит по сканированному паспорту. И видимо, спрос на такие услуги, довольно велик.

Как поступить если мошенники оформили микрозайм на Ваше имя?

Что делать если ситуация уже сложилась:

- Направить иск в судебную инстанцию на банковскую организацию за оформление недействительного микрокредита;
- произвести экспертное исследование подписи в кредитных документах;
- доказать подлог документов.

Как обезопасить свои деньги, зная, что мошенники оформляют микрозаймы даже по ксерокопии паспорта? Несколько практических советов:

1. Берегите свои документы и информацию, которая указана в них от посторонних.
2. Не оставляйте паспорт и его ксерокопии без присмотра. Не стоит доверять свои документы друзьям и знакомым. По статистике, даже родственники совершают подобные махинации.

3. Если друзья, знакомые или родственники попросят разрешение о перечислении денег для них на Вашу банковскую карту. Необходимо созвониться с Вашим банком и уточнить о переводе средств (способ отправки денег и имя либо название отправителя).
4. Хотя бы один раз в год необходимо проверять кредитную историю. Эта проверка осуществляется через бюро кредитных историй (БКИ). Проверку можно заказать по интернету. Нужно учесть, что БКИ несколько, поэтому данные о кредиторской задолженности могут находиться на разных ресурсах.
5. Один раз в год любой гражданин Российской Федерации имеет право на бесплатное получение выписки из кредитной истории (БКИ). Начать лучше из центрального каталога кредитных историй (ЦККИ).
6. Размещение паспортных данных на малоизвестных интернет-сайтах, чревато последствиями. Часто из-за такого несерьёзного отношения граждан к своим документам мошенники оформляют микрозаймы на фиктивные документы.
7. Если Вы потеряли или у Вас украли паспорт, необходимо сразу обратиться в паспортный стол и написать заявление.
8. Внимательно выбирайте посредников, если Вам необходимо содействие при оформлении кредита. Такие услуги оказывают брокеры, репутация этого человека или компании должна быть безупречна. Лучше всего осведомиться отзывами реальных клиентов, а также информацию можно уточнить у профессиональных юристов. Если Вы решились привлечь брокера обязательно заключите с ним договор, при этом тщательно прочитайте все предлагаемые для подписания документы.

Банковские микрокредитные организации во многом сами создают ситуации удобные для мошенников. В погоне за клиентами и прибылью, они настолько упростили оформление кредита и выдачу средств, что каждый желающий может воспользоваться такими услугами».

- **Российская газета – Долги из третьих рук**
  https://rg.ru/2016/08/04/afery-s-oformleniem-lipovyh-kreditov-na-grazhdan-stali-massovymi.html

«Массовыми стали аферы с оформлением кредитов на граждан, которые об этом даже не подозревают

В стране стремительно растет число крайне опасных кредитных мошенничеств – на ничего не подозревающего гражданина кто-то оформляет кредит. Жертва, как правило, узнает об этом спустя месяцы, если не годы из судебной повестки, от приставов или того хуже – от коллекторов. К этому времени приписанная гражданину сумма якобы взятого кредита с огромными процентами за неуплату вырастает многократно. Подобные обманы были еще недавно большой редкостью. Сейчас на фоне финансового кризиса стали массовыми.

На сегодняшний день неизвестно, сколько подобных липовых кредитов было выдано, точнее приписано гражданам. Статистики об обманом оформленных кредитах не существует. Но в полиции, в судах и со слов финансового омбудсмена Павла Медведева, новая разновидность обмана распространяется по стране со скоростью лесного пожара в ветреный день. Полиция и суды таким отдельным подсчетом не занимались. А финансовый омбудсмен сообщил журналистам, что уже каждая четвертая жалоба к нему – о кредите, которого заявители не просили.

"Пальма первенства" в таких обманах, безусловно, у микрофинансовых организаций. Собственно, с них все и началось. Первые мошенничества с кредитами на посторонних граждан обкатали в конторах, которые выдают крохотные займы под чудовищные проценты и практически не требуют документов от заемщиков.

В "Российскую газету" обратилась жительница Волгограда, которой испортили жизнь коллекторы. Она как-то в сложной жизненной ситуации взяла маленький кредит в такой микрофинансовой организации и вовремя его отдала.

Но спустя полгода ей стали чаще всего по ночам названивать взыскатели долгов. Они хамили и угрожали, требуя вернуть якобы полученный, но невыплаченный кредит. Присылали СМС, что пора собирать вещи – за ней уже выехали полицейские, чтобы арестовать.

Попытки связаться с этой микрофинансовой организацией, кстати, расположенной в Москве, ничего не дали. На том конце провода, недослушав абонента, грубо кричали, что деньги надо возвращать и бросали трубку.

Пожилой женщине в местной полиции не помогли – заявление взяли, но отдали участковому, который признаков преступления "не усмотрел".

Справиться с безнадежной ситуацией пенсионерке помогло лишь вмешательство "РГ". В официальном ответе редакции микрофинансовая организация сообщила, что проверила факт и выяснила, что на второй день, после того как гражданка погасила заем, кто-то от ее имени заполнил еще один бланк заявления на кредит. Подпись заемщицы даже подделывать не стали – просто поставили другую. Это женщину и спасло. Финансовая контора ответила редакции, что вопрос закрыт, но кто совершил подлог - неизвестно.

Число таких подписанных неизвестно кем просьб о кредите растет, признали сами руководители этой конторы. Они предпочли не отвечать на вопрос корреспонденту "РГ", чужой человек это сделал или свой сотрудник.

Становится опасным даже реальный и уже давно выплаченный гражданином кредит. Его можно скопировать.

Еще опаснее ситуация с организациями, которые дают кредиты онлайн. Для таких займов от гражданина нужно лишь сканированное фото паспорта. А ваш он или нет – уже неважно. Одному подмосковному доктору потребовался год, чтобы разобраться с 15(!) кредитами, оформленными на нее за двое суток. Откуда у мошенников взялся скан ее паспорта, врач не смогла выяснить – за последнее время копию документа у нее просили в собесе, страховой компании и домоуправлении. В полиции заявление от врача приняли, но ничего делать не стали.

Работают такие фирмы просто – данную в кредит небольшую сумму переводят на карточку нового клиента в один из крупных банков. Тот мошенник, который отправил в микрофинансовую организацию скан чужого паспорта и номер своей карточки, деньги снимает и исчезает. А гражданин, на которого оформлен кредит, узнает о долге тогда, когда сумма из-за штрафов за невозврат становится огромной и просроченный кредит попадает к коллекторам.

Становится опасным даже реальный и уже выплаченный кредит. Его документы мошенники могут "пристроить" в другой банк и по ним получить деньги.

Так, менеджеру фармацевтической фирмы пришел "привет" из службы судебных приставов с требованием погасить долг перед банком, о существовании которого он не догадывался. Его семья действительно взяла кредит на строительство дачи и его выплатила. Но спустя год пришло письмо от приставов.

Оказалось, что копия договора о крупном кредите и все нужные документы попали неведомым образом из одного банка в другой банк. Неизвестно кто вполне профессионально поменял в документах лишь даты и название кредитной организации. Новый банк так и не смог объяснить, кто "одобрил" этот кредит и кому выдали деньги. А семья вынуждена была платить за экспертизу "нового" займа и нанимать адвоката на судебное разбирательство. Которое, к слову, еще не завершилось. Банк категорически отказывается помогать обманутым людям. Полиция отправляет их в суд.

Второй отряд пострадавших от чужих долгов – это те граждане, которые потеряли документы или у них украли паспорт или водительское удостоверение. (По нему микрофинансовые кредиты тоже выдаются.) У кредитных мошенников такой канал использования настоящих документов отлажен великолепно – кредиты по краденым документам оформляются буквально в течение суток. Этот вид обмана опасен тем, что здесь суммы кредитов куда внушительнее. Банки в таких случаях категорически отказываются идти навстречу обманутому человеку, уверяя, что у кредитной организации нет ни полномочий, ни сил, ни времени заниматься расследованием.

Возможно, такая позиция связана с тем, что, по оценке экспертов, в абсолютном большинстве случаев в подобном мошенничестве замешаны сами сотрудники банка. У них есть все реквизиты гражданина, включая скан паспорта и образец подписи. Они даже в суде будут клясться, что лично видели клиента у себя в офисе при подписании договора.

На моей памяти лишь однажды гражданин смог опровергнуть такую ложь, когда предъявил суду свой загранпаспорт с отметкой пограничников, что в день, когда он якобы брал кредит, его в стране не было, и лично приехать в банк он никак не мог.

Справка "РГ"

Как действовать, если на вас оформлен чужой кредит?

Некоторые юристы дают "общие" советы типа бережно относиться к документам и персональным данным. Но это рекомендация из области фантастики. Копии паспортов у гражданина сегодня требуют в огромном количестве предприятий и организаций. Наши персональные данные остаются в страховых конторах, поликлиниках, магазинах при оформлении скидочных карт, в собесах, в управляющих компаниях. Так что тут не уследить. Но вот бежать в полицию при пропаже паспорта надо обязательно. И чем быстрее, тем лучше.

Очень серьезно надо относиться к повесткам или звонкам о долге, даже если точно знаете, что на вас не "висят" невозвращенные кредиты. Обязательно проверяйте такую информацию. Сэкономите нервы и деньги.

В случае если подобное несчастье с липовым кредитом случилось, обязательно обратиться в банк с заявлением в письменном виде, что вы деньги у них не брали. Отправить письмо надо с уведомлением. Оставить у себя копию и квитанцию, что банк

получил письмо. Пусть банк не ответит, но это доказательство в суде. Надо бить во все колокола - полицию, прокуратуру.

Бежать с жалобой к приставам, которые начали забирать ваши деньги, накладывать арест на имущество, бесполезно - они исполняют вступившее в силу решение суда. Так что в битве за честное имя обойти суд не получится. Только здесь могут принять решение, что никаких договоров человек не подписывал и кредитов не брал».

- **Bankiros – ТОП-7 способов мошенничества с кредитами https://bankiros.ru/news/top-7-sposobov-mosennicestva-s-kreditami-701**

«Повышенный спрос на заемные деньги породил множество предложений и стал главной причиной конкуренции финансовых структур. Они упростили процедуры кредитования граждан настолько, что это спровоцировало развитие мошенничества при оформлении и выдаче займов. Рассмотрим самые распространенные виды мошенничества с кредитами и схемы, которые используют злоумышленники.

№1. «Кража личности» или кредит по подложным документам

Большинство займов получено наличными на поддельные или украденные документы. По оценке ОКБ, за предыдущий год в 600 банках было выдано около 70 000 таких кредитов на сумму почти 6,6 млрд. рублей.

Потеря паспорта – первый повод стать жертвой мошенников. Вскоре после случившегося человек может узнать, что на него оформлен потребительский кредит. Обычно злоумышленникам нужны наличные, поэтому ипотека или автокредит маловероятны. Да и проверка службой безопасности банка в этом случае жестче. Однако хлопот и так будет достаточно – всем финансовым организациям станет известно о непогашенном кредите и вас внесут в «черный» список клиентов, а свою непричастность придется доказывать через суд. В «зоне риска» находятся даже те, кто никогда не терял документов – злоумышленнику достаточно знать конфиденциальную информацию, чтобы оформить на человека кредит.

На чужой паспорт злоумышленники умудрялись за короткий срок набрать займов на сумму до 3 млн. руб. Хуже всего то, что их сложно найти и признать мошенниками.

Утверждает Александр Ахломов, RNS-директор по развитию продуктов ОКБ.

Представители Тинькофф банка рассказывают:

Сегодня трудно вычислить злодеев – они настолько качественно могут подделать документы, что даже тщательная проверка при помощи дорогостоящей специализированной техники не всегда дает положительные результаты.

На проблему украденных документов обратили внимание и в Московском кредитном банке. Сотрудники подтвердили увеличившееся число попыток таких махинаций и всеми силами стараются их предотвратить.

В МКБ за год предотвращено 5 попыток взять ипотечный кредит на подложные документы. Общая сумма ущерба, которого удалось избежать, достигла более 15 млн. руб.

Прокомментировал Александр Шорников, директор департамента розничного кредитования МКБ.

Как это предотвратить: Берегите свой паспорт, никому и ни под каким предлогом его не оставляйте. Конфиденциальные данные не разглашайте и не проверяйте вслух.

№2. Кредит другу

Сложная ситуация – когда друг просит стать поручителем, а то и вовсе уговаривает оформить на вас кредит по причине своего несоответствия требованиям банка. Как гласит народная мудрость: «Хотите потерять друга – дайте ему взаймы». Возможно он и будет платить по устным обязательствам, но никто не может быть уверенным в своей платежеспособности на пару лет вперед. Если в один «прекрасный» момент друг перестанет платить кредит, все обязательства лягут на ваши плечи.

Как это предотвратить: Никаких кредитов или поручительств для знакомых. Помните, что чужая душа – потемки. Лучше дайте взаймы и заранее смиритесь с тем, что деньги вам не отдадут.

№3. Семейное мошенничество

Не так давно широкого размаха набрало «семейное» мошенничество, когда кредиты оформляют на родственников. Проблема достигла глобальных масштабов. Во многих банках были выданы кредиты по паспортам однофамильцев или дальних родственников на миллиарды долларов. При этом подозрительных попыток оформления кредитов с использованием чужих документов зафиксировано еще больше. Злоумышленники в этом случае действуют по четкой схеме: они под видом родственника (схожесть зачастую очевидна) стараются набрать как можно больше кредитов в разных организациях одновременно.

Как это предотвратить: Никогда не давайте своих документов даже людям, которым доверяете.

№4. Ложные схемы при оформлении экспресс-кредитов в магазинах

Множество торговых сетей предлагает приобрести товары в кредит. Мошенники добрались и до них. Схема в этом случае заключается в обмене купленной техники на наличные. Например, человек решил приобрести плазменный телевизор, стоимостью 100 тыс. рублей. В момент оформления кредита к нему подходит «посредник» и предлагает выкупить технику за 30-50 тыс. + обещает выплачивать кредит, но просит внести первоначальный взнос в размере 10 тыс. То есть, жертва получает 30-50 тыс. на руки и забывает о кредитном договоре. Однако потом посредник исчезает, а клиент остается без телевизора, за который банк требует уплатить по просроченному займу полную сумму с процентами. В такой ситуации доказать факт мошенничества практически невозможно – на документах стоят подписи клиента.

Александр Воронин, директор департамента потребительского кредитования Русфинанс Банка рассказывает:

«Тренд на мошенничество при оформлении кредита на бытовую технику растет. Обычно к схеме привлекают сотрудников магазинов, которые оформляют ссуды на товар, используя фальшивые данные либо клиентов в сопровождении «перекупщиков». Чаще всего выбирают товары, которые можно быстро продать – мобильные телефоны, ноутбуки. Чтобы предотвратить подобные ситуации, мы стараемся направлять в торговые точки своих сотрудников. За год выявлено 185 подобных заявок, ни одна из которых не была одобрена.»

Как это предотвратить: Не верьте людям, обещающим платить за вас кредит. Отсутствие договора на посредническую деятельность – первый признак, что к вам обратились мошенники. Не соглашайтесь на получение легких денег, так как придется отдавать гораздо больше. Лучше откажитесь от покупки, которую не готовы оплатить или найдите, у кого занять денег.

№5. Мошенники среди сотрудников кредитной организации

Увы, мошенничество с кредитами в банках встречается довольно часто. Здесь возможно не менее пяти схем. Иногда недобросовестные сотрудники организации содействуют преступникам или состоят с ними в сговоре, но чаще всего идут на хитрость: размещают объявления о «быстром кредите без справки о доходах». Как только человек обращается и отдает паспорт для заключения договора, аферисты на его имя оформляют несколько кредитов. Нередко требуют предварительно оплатить определенную сумму «за выпуск карты». Затем паспорт возвращают, ссылаясь на невозможность выдачи займа по весомой причине. Спустя некоторое время мошенники скрываются, а доверчивому клиенту от банков приходят письма о необходимости погашения просроченных кредитов, о которых он и не подозревал.

Как это предотвратить: Не обращайтесь к неизвестным частным лицам за помощью и не платите за услуги заранее. О паспорте уже упоминалось в первом пункте.

№6. «Черные брокеры»

Это третьи лица, готовые пойти на обман банка, чтобы получить вознаграждение за полученный человеком кредит. Они предлагают документы с ложной информацией о заемщике. Как правило, такой «брокер» способен подделать для клиента справку о доходах и даже подтвердить данные о несуществующем месте работы. Но подобные шутки заканчиваются плохо – служба безопасности банка быстро выявляет несоответствие, брокер исчезает, а заемщик портит себе кредитную историю и может впоследствии попасть под административное или уголовное делопроизводство.

За предыдущий год было зафиксировано несколько случаев «посредничества» при выдаче займов в Юникредит банке. Как рассказали руководители:

Ипотечные брокеры, менеджеры автосалонов и другие партнеры зачастую «подтягивали» профиль заемщика под стандарты банка или фальсифицировали часть документов.

Как это предотвратить: Ведите честную «игру» с банками, чтобы не испортить свою кредитную историю и бегите от черных брокеров подальше.

№7. Новый жесткий метод мошенничества на отечественном рынке кредитования

В 2017 г. зафиксированы случаи, когда нелегальные фирмы обманным путем принуждали граждан одновременно с кредитным договором подписать документ о покупке-продаже недвижимости. Это подтвердили официальные представители пресс-службы ФНП. По их мнению, злоумышленники уповали на невнимательность людей, так как их жертвами обычно становились пенсионеры, нуждающиеся в деньгах (им проще подсунуть для подписи нужные бумаги). Преступники уже «засветились» в Москве, Подмосковье, Карелии, Хакасии, Смоленске, Свердловской области, Химках, Сочи. Количество пострадавших достигло до сотни. К сожалению, среди мошенников

присутствуют не только нелегалы, но и микрофинансовые организации, которые входят в реестр ЦБ.

Злоумышленники действуют по схеме: размещают объявления о кредите на крупную сумму под минимальный процент. Когда человек обращается, ему дают на подпись множество документов, разобраться в которых без познаний в юридической сфере невозможно. При этом кредиторы торопят клиента, ссылаясь на время, и он быстро все подписывает. О том, что среди бумаг был договор о продаже квартиры, жертва узнает позже, – когда представители кредитора являются с требованием покинуть жилплощадь.

Виктор Климов, руководитель проекта ОНФ «За права заемщиков» поясняет, что:

После подобного шага у заемщика мало шансов доказать, что его обманули. Защитить жертву в такой ситуации практически невозможно – судьи опускают руки, так как человек лично подписал документы на продажу.

Денис Герасимов, партнер адвокатского бюро RBL, рекомендует:

«Пострадавшим гражданам следует подать иск о признании сделки по продаже жилья недействительной до того, как новоиспеченный собственник снимет его с кадастрового учета. Ссылаться при этом нужно на свой непрофессионализм. Несоответствие суммы по договору и фактической стоимости недвижимости послужит весомым аргументом.»

Как это предотвратить: Вычитывайте каждый документ, который вам дали на подпись. Если не понимаете, о чем там речь, обратитесь за помощью к юристу.

Как избежать риска стать жертвой мошенников

Мы рассмотрели лишь мизерную часть возможных способов мошенничества с кредитами. Чтобы не попадаться на уловки злоумышленников, важно не пренебрегать мерами безопасности, уделять внимание собственной финансовой грамотности и в любой ситуации быть крайне бдительным.

Перечислим 6 «золотых» правил, которые помогут избежать махинаций с кредитами:

1. Проверьте рейтинг выбранной финансовой организации. Информацию можно получить от знакомых, посетителей, из интернета (отзывы, форумы, справочники). Если у кредитора нету сайта и офиса – уходите, так как у приличных компаний есть и то, и другое. Обратите внимание на способ связи – если контактных данных мало, не связывайтесь с этим кредитором.
2. Не доверяйте свои документы даже близким людям и не разглашайте личные данные. Копии паспорта или удостоверений личности также не оставляйте в неизвестных организациях (кроме случаев, предусмотренных законодательством).
3. Следите за документами, которые подписываете – оформление дополнительного займа по подложным договорам является уголовным преступлением.
4. Если вам навязывают страхование при оформлении кредита, знайте, что согласно законодательству, у каждого клиента есть право отказаться от страховки без объяснения причин.
5. В случае потери паспорта сразу подавайте заявление в органы ГУВМ МВД.

6. Чтобы избежать «чужих» займов, контролируйте собственную кредитную историю. Например, периодически запрашивайте отчет с бюро кредитных историй или закажите услугу SMS-оповещения о любых изменениях – запрос личных данных, выдача кредита на ваше имя и др.

Повышенное внимание к личной конфиденциальной информации и подписываемым документам поможет избежать плачевных последствий от деятельности кредитных мошенников.

Александр Сагин, начальник юридического отдела ФНП предупреждает, что:

«Застраховаться от мошенников можно лишь одним способом – не спеша вычитывайте все бумаги, которые будете подписывать. А еще лучше, берите их для детального ознакомления домой. Если это не допустимо в данной организации, тогда попросту разворачивайтесь и уходите, поскольку честным кредиторам нечего скрывать. Когда требуется предоставить жилье в качестве залога, сначала проконсультируйтесь с квалифицированным специалистом, чтобы избежать роковой ошибки. При выявлении чужой подписи на кредитном договоре, оформленном на ваше имя, требуйте проведения почерковедческой экспертизы и записи с видеокамер наблюдения.»

Что делать тем, кто уже попался на уловки злоумышленников?

Человек, который стал объектом необоснованных претензий со стороны банка, может попытаться решить проблему в рамках законодательства. Главное – доказать, что он оказался жертвой мошенников, и деньги не получал (кредитный договор вступает в силу только после принятия средств). При этом нет смысла убеждать сотрудников финансовой организации в своей невиновности, лучше выполнить следующие действия:

Шаг 1. Потребовать у банка копию договора, чтобы ознакомиться с подписями лжезаемщика и предоставленными данными. Подтвердить непричастность клиента, на документы которого оформлен кредит, можно в случае использования недостоверной информации, а также при помощи графологической экспертизы. Этого достаточно, чтобы снять все обвинения.

Шаг 2. Написать на имя руководства банка претензию, указав объективную причину, подтверждающую невозможность получения вами кредита (потеря документов, отъезд, устаревшие данные).

Шаг 3. Обратиться в отделение милиции с заявлением о возбуждении дела по статье «Мошенничество», поскольку кредит оформлен злоумышленниками, а возмещения банк требует от вас.

Шаг 4. Если кредитор подал иск о возврате займа, надо подготовиться к судебному процессу и сопутствующим затратам. После признания виновности банка средства будут возмещены (включая моральный ущерб от вымогательств и звонков).

Юрист Александр Дондоков рекомендует потерпевшим от кредитного мошенничества:

«Нужно тесно сотрудничать с правоохранительными органами и судом, обращаться к органам предварительного следствия и требовать изъятия у банка материалов, подтверждающих вашу невиновность (например, записи видеокамер)».

Как банки борются с мошенничеством

Известные финансовые организации вводят дополнительные схемы распознавания мошенничества при получении кредита, используя:

- системы скоринга;
- биометрические параметры;
- бюро кредитных историй;
- внешние источники информации;
- социальные сети.

Эти методы помогают на стадии оформления кредита значительно сузить круг подозрительных личностей. При выявлении злоумышленников данные передают в правоохранительные органы.

В МКБ для распознавания и предотвращения мошенничества внедрили антифрод-системы, задействовали операторов мобильной связи и намерены активно применять биометрию.

В Юникредит банке утверждают, что используют собственные схемы для выявления мошенничества и повышения качества работы партнеров-продавцов с целью защиты репутации банка.

Для борьбы с мошенничеством на национальном уровне банки объединяются в организацию «Национальный Хантер», где насчитывается уже более 50 участников. При оформлении займов они перенаправляют заявки для обработки на платформе Hunter. Программа сравнивает информацию, определяет недостоверные данные и совпадения с мошенническими схемами. Это уже помогло предотвратить попытки махинаций на сумму свыше 50 млрд. руб.

И главное – Росфинмониторинг предоставляет списки подозрительных заемщиков Центральному банку России, который передает их кредитным организациям. Все это дает надежду на то, что в будущем случаи мошенничества будут постепенно сокращаться».

2.2. Информация о случаях оформления кредита по чужим документам, с комментариями экспертов

Здесь собраны истории о конкретных ситуациях, рассказанные участниками журналистам или в интернет-форумах:

- **Аргументы и факты – Паспорт чужой – деньги мои. Как кредитные аферисты берут займы**
  http://www.aif.ru/society/safety/pasport_chuzhoy_dengi_moi_kak_kreditnye_aferisty_berut_zaymy

«Житель Соликамска случайно узнал, что должен банку 40 тысяч рублей. Как оказалось, директор фирмы, которая оказывала помощь в кредитовании, воспользовался его паспортными данными и оформил заем, минуя владельца.

Кредит не брал, но долг плати

Когда у Сергея П. (имя изменено – прим.ред.) сложилась трудная финансовая ситуация, он попытался обратиться в банк за займом. Но в Соликамске, где проживает Сергей, ему везде отказывали в получении кредита. Мужчину это очень удивило, ведь

несколько лет назад, когда ему также срочно потребовалась крупная сумма денег, взять кредит было гораздо проще.

«В чём дело, было непонятно. Думал, может, нужно снова в специальную фирму обратиться за помощью», – вспоминает Сергей.

Специальная фирма, о которой он говорит, – это компания-посредник, оказывающая содействие людям при получении кредита. Именно эта фирма (а точнее, её экс-руководитель) и была причиной трудностей Сергея.

Мужчине удалось выяснить, что постоянные отказы он получает из-за испорченной кредитной истории. При этом последний заем он вернул в срок и в полном объёме, а оформленный летом 2016 года в одной из микрофинансовых организаций кредит он вообще не брал. Тогда Сергей обратился в дежурную часть межмуниципального отдела МВД России «Соликамский».

Сотрудники полиции нашли виновника. Им оказался бывший сотрудник фирмы-посредника, в которую несколько лет назад обращался Сергей. Выяснилось, что он уже был судим. 39-летний злоумышленник в 2012 году был руководителем фирмы, помогающей клиентам получать кредиты, поэтому у него был доступ к персональным данным обратившихся.

Летом 2016 года он столкнулся с финансовыми трудностями и решил воспользоваться копиями паспортов, которые у него сохранились. Мужчина обратился в одну из микрофинансовых организаций, где представился Сергеем П. Заявка на заем оформлялась через интернет, а деньги перечислялись на счёт. Преступник указал паспортные данные и место работы Сергея, а электронную почту, номер телефона и счёта – свои.

В результате заявка прошла проверку и 20 тыс. рублей, которые взял в кредит аферист, отправились к нему. Возвращать заем он, разумеется, не планировал. Спустя почти год сумма долга увеличилась в два раза и настоящий Сергей П. оказался должен МФО уже 40 тыс. рублей, о чём он неожиданно узнал, когда ему самому потребовался кредит. Сергей не узнал бы об этом, если бы сам не обратился в банк. Он долгое время проживает не по месту регистрации, поэтому все звонки на домашний телефон и визиты коллекторов прошли мимо него.

Сам помог мошенникам

Сергею в каком-то смысле даже повезло: преступник, воспользовавшийся его персональными данными, проживает в том же городе, что и он. В ряде случаев подобного мошенничества жертва и злоумышленник могут находиться в разных концах страны, а это значительно затрудняет поиск преступника.

Оказывается, стать жертвой такого «микромошенничества» не так уж сложно. Злоумышленнику для получения кредита в микрофинансовой организации нужны только паспортные данные. Даже личное присутствие при оформлении займа не потребуется. Это значительно облегчает мошенникам деятельность. Им не нужно искать настоящие документы жертвы или их копии, гримироваться так, чтобы походить на фото в паспорте.

Некоторые аферисты пользуются служебным положением, как это произошло в случае с Сергеем. Другие не занимаются этим регулярно, но случайно найденный паспорт

провоцирует их на преступную деятельность. Нередко отсканированные документы оказываются в свободном доступе в социальных сетях. Взломанная электронная почта с привязанным к ней облачным хранилищем, где есть копии документов, тоже может стать находкой для мошенника. Иногда люди, нашедшие чужие документы, выкладывают фотографии в соцсети, чтобы найти хозяина, сделав тем самым доброе дело, но помогают они преступникам.

По данным ГУ МВД РФ по Пермскому краю, только в этом регионе за 2017 год выявлено 359 преступлений в кредитно-финансовой сфере. Аферист, который воспользовался данными Сергея П. и испортил ему кредитную историю, был признан виновным. Суд приговорил его к 7 месяцам исправительных работ с удержанием 10% из заработной платы в доход государства.

Гороскоп подсказал

АиФ.ru решил проверить, насколько сложно получить заем через интернет. Оказалось, что мошеннику в таком деле неплохо помогает знание гороскопа, а точнее, знаков зодиака.

Сначала пробуем выяснить, что потребуется для кредита через интернет, позвонив на «горячую линию» выбранной случайным образом МФО. Сотрудница call-центра сообщает, что нужен только паспорт. При этом личное присутствие не требуется: «В вашем регионе есть два офиса, – в Перми и в Березниках – но оставить заявку можно на сайте или по телефону нашим специалистам», – сообщает девушка.

Кроме того, выясняется, что проверка данных, которые предоставляет потенциальный заёмщик, происходит в автоматическом режиме, то есть без участия человека.

– Если вы оформляете заявку через наш сайт, – сообщает сотрудница МФО, – то сразу после оформления вы увидите, одобрен ли вам кредит.

– Мне после этого позвонят?

– Могут и не перезвонить.

– Что будет, если кредит не одобрят? Я узнаю о причинах?

– Нет, такая информация не сообщается.

Девушка уверяет, что никаких ошибок при проверке паспортных данных, которые мы предоставим, не случается. Более того, можно быть уверенным в своей безопасности, ведь личная информация третьим лицам не передаётся.

Единственное, где мошенник может «засветиться», – это при получении займа, так как для этого нужно прийти в офис компании, занимающейся переводами. Но в других подобных МФО предоставляется широкий выбор способа получения: начиная от банковской карты и заканчивая электронными кошельками, которые можно оформить на любые паспортные данные.

В онлайн-заявке указываем данные паспорта и место работы другого человека. Почту создаём такую, чтобы было непонятно, кому она принадлежит. Счёт также оформлен на другое лицо. После того, как заявка была оформлена, предварительное одобрение получено, на указанный в форме номер перезвонили. Уточняли детали (зачем нужен заём,

как скоро планируется вернуть деньги) и попросили вновь назвать паспортные данные. А затем прозвучал неожиданный вопрос:

– Ваш знак зодиака?

– Скорпион!

– Спасибо, ваша заявка одобрена. Готовы получить перевод на счёт?

Видимо, вопрос, заданный специалистом МФО, должен помочь определить, действительно ли именно владелец паспорта пытается получить заём...

«Паспорт не терял, деньги не получал»

Случаи мошенничества в сфере кредитования нередки, а потенциальной жертвой может стать любой, кто хоть раз где-либо оставлял свои паспортные данные. Нередко пострадавшие, не выдержав постоянных звонков и визитов коллекторов, готовы отдать чужой долг, лишь бы их оставили в покое.

«Если вы узнали, что у вас есть долг по кредиту, который не брали, то нужно запросить кредитную историю и отчёт в этой организации, чтобы знать количество займов, точную сумму и накопившиеся проценты, – советует ассистент кафедры теории и истории государства и права Пермского государственного национального исследовательского университета Мария Лысачкова. – После этого следует подать заявление в полицию, где нужно подробно написать, что случилось, кто, по-вашему мнению, мог использовать данные паспорта и взять кредит. Важно не забыть документ с отметкой о принятии заявления.

Следом нужно отправить в организации, где взяты кредиты, письма с приложенным заявлением в полицию заказным письмом Почтой России с уведомлением о вручении. Скан письма можно продублировать по электронной почте. Если это был заем в банке, то можно обратиться в суд, назначить почерковедческую экспертизу, запросить фотографию, так как многие банки сейчас фотографируют клиентов. Если кредит брали через интернет, это сложнее, там даже подпись нельзя проверить. Но если деньги по такому займу переводили на карту, то можно взять выписку со счетов, подтверждающую, что данная сумма в такой-то период вам не поступала. Если коллекторы требуют возврата долга, то нужно направить им копию заявления в полицию. Если не перестанут звонить – пригрозить жалобой в Федеральную службу судебных приставов. Если дело всё же дошло до вмешательства приставов, то следует обратиться в суд для приостановления исполнительного производства. Кроме того, деятельность МФО попадает под оказание услуг, следовательно, на их действия можно пожаловаться в Роспотребнадзор. Напишите жалобу на то, что данная организация без проверок выдаёт кредит на ваше имя и без вашего ведома, хотя вы ничего не подписывали, паспорт не теряли и деньги не получали».

- **Banki.ru – из сообщений на Форуме https://www.banki.ru/forum/?PAGE_NAME=read&FID=61&TID=269237**

«Год назад на мой паспорт был оформлен кредит на покупку бытовой техники через банк "Ренессанс кредит". О данном кредите я узнала, когда по почте на мой адрес пришло информационное письмо и график платежей. В этот же день я обратилась и в банк и в милицию с заявлениями. Самое странное, что паспорт мой был дома в целости и сохранности. Пол года служба безопасности банка и милиция вели параллельные

расследования. Итог мероприятий был вообще неожиданным. В банке пришли к выводу что я ЛИЧНО оформила кредит и потребовали его платить. В то время, когда сотрудник банка мне об этом сообщал, в милиции уже нашли девушку, которая совершила эту сделку, и она давала признательные показания. Оказалось, что это была моя знакомая, которая за месяц, как я узнала о кредите, брала у меня паспорт, под предлогом приобретения сим карты, а потом просто вернула документ (через 30 минут). (к слову - этому человеку я всецело и всегда доверяла) В последствии у нас была очная ставка в милиции, на которой девушка еще раз признала свою вину. Дознаватель, которая вела мое дело направила документы в прокуратуру, после чего от туда пришел ОТКАЗ в возбуждении уголовного дела в отношении моей знакомой, так как она на тот момент платила кредит (следовательно, сточки зрения правоохранительных органов, умысла на хищение и присвоения денежных средств и имущества не имела). Но в отказе тем не менее, было указано и расписано, при каких обстоятельствах и кем на самом деле был оформлен кредит. Мошенничеством не является! Прошел год. Платить она перестала - уже около трех месяцев. Активизировался банк, звонят каждый день, и робот и люди. Две недели назад я повторно написала в банк заявление, к которому приложила копию документа с ответом из прокуратуры. Сегодня 8 человек по счету из Ренессанса мне позвонил и предложил заниматься выбиванием денег из той девушки самостоятельно, пояснил, что даже при уплате ей всех денежных средств, моя кредитная история исправляться не будет. Я в растерянности, и не знаю что мне делать. Ждать когда банк подаст на меня в суд, (а они могут и не подать, если она возобновит платежи) или подавать на признание сделки недействительной самостоятельно? Обязаны ли они мне будут возместить все финансовые издержки на адвоката, почерковедческую экспертизу (и нужна ли она, если есть показания признательные) и т.д. Я в растерянности, и не знаю что мне делать. Я ни разу в жизни не брала никаких кредитов, а теперь моя кредитная история испорчена, и очень портят нервы звонки из банка. Помогите советом».

- **РБК – По чужим долгам: как живут люди с оформленными на их имя кредитами**
  https://www.rbc.ru/money/28/07/2016/5798f77f9a79474c527b90fb

«Как быть, если на вас оформили кредит, который вы не брали? РБК собрал три истории людей, пострадавших от кредитных мошенников.

Статистики по количеству незаконно оформленных на граждан кредитов нет. Но, по словам финансового омбудсмена Павла Медведева, эта проблема довольно распространена. Жалобы на такого рода мошенничество и возникающие из-за этого проблемы занимают четвертое место среди всех обращений в его приемную. С кризисом число пострадавших от кредитных мошенников растет, заметил Медведев: особенно часто в таких историях упоминаются микрофинансовые организации (МФО), которые не так тщательно проверяют заемщиков, как банки.

Если вы оказались жертвой мошенников, оформивших кредит по вашим документам, стоит готовиться к звонкам коллекторов, длительным судебным разбирательствам, потере времени и денег. РБК собрал три таких истории, чтобы на их примере показать, как правильно действовать, если на ваше имя оформили кредит.

По кредиту в день

В 2015 году заместитель управляющего бизнес-центром Сергей Овчинников узнал, что стал должником сразу четырех микрофинансовых организаций. В июле 2015 года ему позвонили из МФО «Е заем» и сообщили, что с учетом набежавших процентов необходимо выплатить 15 тыс. руб. Изначальная сумма займа составляла 6 тыс. руб., оформлен он был якобы в апреле 2015 года.

Еще через несколько дней позвонили из МФО «Займер». Там в апреле 2015 года на него также был оформлен микрозаем на 1 тыс. руб. Спустя несколько недель пришло уведомление от компании Pay P.S. (МФО «Онлайн Займ») – там он якобы взял 4 тыс. руб., тоже в апреле. Четвертый звонок, который совсем уж встревожил Овчинникова, был от компании «Лайм-Займ»: сам того не зная, он оказался должен этой фирме 61 тыс. руб. с учетом процентов.

Все эти займы объединяет одно – они были оформлены онлайн, с использованием его паспортных данных. Каждый день (с 24 по 27 апреля 2015 года) на него оформляли по одному микрокредиту. «В «Е заем» рассказали, что деньги были переведены на карточку Сбербанка», – рассказывает пострадавший. При этом, по его словам, он не является клиентом этого банка.

Получив первое сообщение о долге, Овчинников обратился к участковому, а также написал заявление в полицию. С получением каждого уведомления о долге он писал новое заявление, но пока никаких новостей от полиции по его делу нет

Овчинников, по его словам, выплачивает автокредит в Меткомбанке. Кроме того, у него есть кредитная карта банка «Уралсиб», по которой ни разу не было просрочек. «Паспорт я никогда не терял, он всегда со мной», – недоумевает он. Расстраивает Овчинникова и то, что его жене, пытавшейся оформить кредит в банке, отказали из-за его плохой кредитной истории. Кроме того, спустя некоторое время ему стали звонить коллекторы, требуя вернуть деньги по самому крупному «долгу» в компании «Лайм Займ». «Ни одной копейки жуликам платить не буду», – упирается Овчинников.

Есть множество способов завладеть паспортными данными для получения кредита, считает старший юрист фирмы «ЮСТ» Владимир Бояринов: достаточно просто оставить документ где-то на время. При этом Бояринов не понимает, как МФО может выдать заем только лишь по паспортным данным. Генеральный директор компании «Займер» Сергей Седов уверяет, что его компания подтверждала личность этого заемщика, задавая вопросы по кредитной истории, ответы на которые не мог знать посторонний человек.

Управляющий директор сервиса онлайн-кредитования «Е заем» Лига Трупа утверждает: таких ситуаций, когда мошеннику удается взять кредит по чужим паспортным данным, очень мало. По скоринговой модели этой компании, прежде чем выдать заем, оцениваются в том числе кредитная история «Е заем», данные трех БКИ, а также информация о том, как потенциальный заемщик платил за связь, рассказывает она. Впрочем, Трупа признает, что иногда мошенникам удается обойти проверку. В этом случае «Е заем» передает информацию в полицию. Похожей схемой пользуется и «Займер», рассказывает его директор Сергей Седов. Он также утверждает, что подобных случаев немного: около 0,2% от общего количества выданных займов.

Что говорят юристы:

«Овчинникову стоит направить во все МФО, где оформлен заем, письма о том, что он не оформлял никаких кредитов», – советует Бояринов из «ЮСТ». Также он предлагает запросить у МФО копии договоров займа. Даже если они останутся без ответа, легче будет подтвердить добросовестность человека, если дело дойдет до суда, уверен Бояринов.

По его словам, в этой ситуации имеет смысл не дожидаться новых попыток коллекторов взыскать долг и самостоятельно обратиться в суд. Первое требование – признать договор займа незаключенным, второе – обязать МФО направить в БКИ информацию об аннулировании записи о задолженности, говорит Бояринов. Возможно, Овчинникову не придется воспользоваться этим советом. По его словам, сотрудники «Е заем» связались с ним сразу же после звонка из РБК и пообещали прекратить взыскание долга, а также восстановить его кредитную историю.

Суд с Альфа-банком

В мае 2013 года менеджер из Москвы Елена Кислова неожиданно получила СМС-сообщение из Альфа-банка. В нем говорилось, что она якобы оформила в торговой точке кредит на сумму 100 тыс. руб. У Кисловой был счет в этом банке, она исправно, по ее словам, выплачивала небольшой кредит.

Новый кредит, который был оформлен без ее участия, девушку озадачил. Кислова написала претензию в банк и заодно обратилась в полицию. «Ходила в банк раз в неделю, подавала заявления, они визировали их и ставили отметку, что приняли», – рассказывает Кислова. Альфа-банк ей не ответил, а в полиции не помогли.

В сентябре Кислова улетела в Италию, где собиралась отпраздновать свое 30-летие. В день рождения на нее посыпались звонки банка с требованием вернуть долг. «Операторы говорили наглым тоном, как с преступницей, испортили весь отдых, – с обидой вспоминает она. – И это после того, как я ходила к ним с письмами и упрашивала их разобраться».

Вернувшись в Россию, Кислова первым делом нашла адвоката и подала на банк в суд. К началу разбирательства сумма долга выросла до 105 тыс. руб. за счет набежавших штрафов за просрочку. Суд длился полгода – до марта 2014 года. «Каждый месяц я ездила на заседания», – рассказывает Кислова.

Решение суда признало правоту Кисловой: кредит она не брала. По решению суда банк должен был выплатить компенсацию, которая совпала с записанным на клиента долгом – 105 тыс. руб. (45 тыс. руб. – расходы на адвоката, 40 тыс. руб. – моральный ущерб, 20 тыс. руб. – штраф).

Пресс-служба Альфа-банка сообщила РБК, что подобные ситуации происходят редко. «У банков нет полномочий и соответствующих ресурсов проводить какие-либо следственные мероприятия по фактам предполагаемого мошенничества. Это исключительные функции следственных органов», – сообщила пресс-служба. Официальная позиция банка – сожаление по поводу того, что мошенники могут использовать в том числе достаточно профессионально подделанные документы при получении кредитов.

Что говорят юристы:

Подобные истории, когда мошенники оформляют в банке кредит на имя одного из клиентов банка, также довольно распространены. «Случаев масса, а суть одна – обычно замешаны сотрудники самого банка и требуется внутреннее расследование», – говорит адвокат Александр Карабанов. С ним согласна и адвокат Московской областной коллегии адвокатов Ирина Зуй. По ее словам, в 90% таких случаев замешаны сами сотрудники банка. По ее словам, в банке есть все необходимые данные заемщика, а подпись можно подделать.

По старому паспорту

В 2006 году москвичка Динара Садретдинова вышла замуж, взяла фамилию мужа и сдала свои старые документы в паспортный стол. Спустя четыре года женщина узнала, что на старый паспорт с девичьей фамилией в 2010 году был оформлен кредит в ОТП Банке. Садретдинова якобы накупила в долг электроники и бытовой техники на 100 тыс. руб., причем заказ на покупку был оформлен онлайн.

В течение следующих трех лет из банка периодически приходили письма, которые женщина с чистым сердцем отправляла в мусорную корзину: по ее словам, ни одного кредита в жизни она не брала. Но в 2014 году ей пришла повестка в суд, и проблему все же пришлось решать. Ее вызвали свидетелем по делу о мошенничестве. Выяснилось, что группа мошенников, заполучив чужие паспорта и переклеив фотокарточки, оформляла в московских магазинах кредиты на покупку товаров. Таких пострадавших, как Садретдинова, было около десяти человек. Всего мошенники оформили на граждан кредитов на 1 млн руб. В 2015 году после судебного разбирательства им дали по пять лет тюрьмы.

Однако на этом история не закончилась. Через полгода после суда Садретдиновой ее мужу и брату начали звонить коллекторы. За это время сумма долга с учетом процентов выросла до 283 тыс. руб. Сейчас женщина ждет ответа от банка, в который она подала жалобу.

Как сообщила РБК пресс-служба ОТП Банка, из-за длительных неплатежей договор с Садретдиновой был передан в работу коллекторам, а в конце 2015 года продан в составе пула плохих долгов. Банк утверждает, что клиент впервые обратился к ним только в июле 2016 года и предоставил не все необходимые для урегулирования проблемы документы. «Клиенту было направлено повторное уведомление о необходимости предоставить полный пакет документов, включая решение суда и копии всех страниц паспорта. До сих пор эти документы банк так и не получил», – сообщила пресс-служба банка. Как только это будет сделано, банк обещает разобраться, остановить процедуру взыскания долга и стереть данные о нем из бюро кредитных историй.

Что говорят юристы:

Адвокат московской коллегии адвокатов «Князев и партнеры» Зиннур Зиннятуллин (он же адвокат по этому делу) рассказывает, что фактов утери или хищения паспорта в этой истории нет – он был передан в паспортный стол для замены в связи со вступлением в брак и изменением фамилии. А генеральный директор компании «Правокард» Станислав Каплан уверен, что такая ситуация могла произойти только при участии сотрудников паспортного стола либо в результате кражи документов из этого учреждения.

Президент Ассоциации корпоративного коллекторства Дмитрий Жданухин говорит, что если кредитная организация, обладая информацией об этом деле, продолжит требовать

деньги с героини истории, это тоже может расцениваться как мошенничество (ст.159 УК РФ). «Иными словами, если банк предупрежден и получал жалобы от гражданина, но продолжает требовать деньги и даже подает в суд, скрывает факт обращений гражданина, в некоторых случаях это квалифицируется как мошенничество», – утверждает Жданухин. Чтобы это доказать впоследствии, необходимо максимально быстро представить банку или коллекторам информацию о смене или утрате паспорта, говорит Жданухин. «Однако обычно дело в такую плоскость не переходит, и суд просто отказывает во взыскании долга», – подчеркивает Жданухин.

Как действовать, если на вас оформили кредит

Первое, что необходимо сделать, – немедленно обратиться в банк. «Сразу же направляйте заявление, что вы не брали никакого кредита, а также требование провести внутреннее расследование», – советует адвокат Московской областной коллегии адвокатов Ирина Зуй. Также стоит написать заявление о возбуждении уголовного дела в полицию. «Пусть правоохранительные органы также займутся этим делом», – советует адвокат Александр Карабанов.

Если банк не боится проверок и не идет на уступки, стоит привлечь юриста и составить вместе с ним исковое заявление. «Также можно обратиться с заявлением в Центральный банк и прокуратуру», – советует генеральный директор компании «Правокард» Станислав Каплан. «Последовательно отстаивайте свою позицию, – призывает Зуй. – Если мирно вопрос урегулировать не получится, судитесь с банком».

2.3. Проблемы расследования кредитного мошенничества, судебные решения, юридические консультации

Проблемам расследования случаев кредитного мошенничества правоохранительными органами посвящены следующая статья:

- **Атаманов Р.С. Некоторые вопросы расследования мошенничества в сети интернет. Статья доступна по ссылке: https://cyberleninka.ru/article/n/nekotorye-voprosy-rassledovaniya-moshennichestva-v-seti-internet**

Возможно, интересны будут также следующие статьи, анализирующие инструментарий аналогичных расследований:

- **Егерев И.М., Ковригина Г.Д. Типичные следы мошенничества, совершаемого в финансовой сфере, и их криминалистическое значение. (Ссылка: https://cyberleninka.ru/article/n/tipichnye-sledy-moshennichestva-sovershaemogo-v-finansovoy-sfere-i-ih-kriminalisticheskoe-znachenie);**
- **В.В. Лысенко. Особенности расследования мошенничеств в сфере кредитования в условиях противодействия и его преодоления. Статья доступна по ссылке: https://cyberleninka.ru/article/n/osobennosti-rassledovaniya-moshennichestv-v-sfere-kreditovaniya-v-usloviyah-protivodeystviya-i-ego-preodoleniya.**

В гражданском судопроизводстве обязанность доказывания лежит на сторонах – истце и ответчике. Согласно Статье 56 Гражданского процессуального кодекса (http://base.garant.ru/12128809/2b6ebde936316453fb0f8db9c6ad7e2c/), каждая сторона

должна доказать суду те обстоятельства, на которые она ссылается как на основания своих требований и возражений.

Поэтому в отсутствие убедительных для суда доказательств непричастности человека к получению кредита решение, подтверждающее это, принято не будет.

Ситуация усугубляется попытками мошенничества со стороны недобросовестных заемщиков, не признающих получение кредита при нежелании (или невозможности) его выплачивать.

Ниже приводятся некоторые судебные решения по искам граждан, отрицающим наличие договорных отношений с кредитором:

- **Определение Судья Матвиенко О.А. Судья-докладчик Иванова О.Н. по делу № 33-5387/2018**

АПЕЛЛЯЦИОННОЕ ОПРЕДЕЛЕНИЕ

26 июня 2018 года г. Иркутск

Судебная коллегия по гражданским делам Иркутского областного суда в составе:

судьи-председательствующего Гуревской Л.С.,

судей Шовкомуда А.П. и Ивановой О.Н.,

при секретаре Шистеевой Н.А.,

рассмотрев в открытом судебном заседании гражданское дело по иску Варламовой Е.В. к обществу с ограниченной ответственностью Микрофинансовая компания «КОНГА» о взыскании компенсации морального вреда, судебных расходов, обязании убрать из кредитной истории имеющиеся записи

по апелляционной жалобе Варламовой Е.В. на решение Октябрьского районного суда города Иркутска от 5 февраля 2018 года по данному делу,

УСТАНОВИЛА:

в обоснование заявленных требований истец указал, что начиная с (дата изъята) истцу на мобильный телефон стали поступать звонки от агрессивных граждан, представившихся сотрудниками отдела взыскания задолженностей ООО МКК «КОНГА». Данные лица вымогали у нее денежные средства, которые якобы являются ее задолженностью перед микрокредитной организацией.

Вместе с тем, истец никогда не брала займов или кредитов у организации-ответчика, договоров с ними не заключала, до этого момента не знала о существовании такой кредитной организации. Она неоднократно указывала сотрудникам ООО МКК «КОНГА» на указанные обстоятельства, однако звонки так и не прекратились.

Истец нашла в сети Интернет сайт данной организации, позвонила по указанному на сайте контактному телефону и проинформировала менеджера о имеющейся проблеме. Ей устно обещали провести проверку и оградить ее от необоснованных звонков. Однако обещание не было выполнено. При этом разговоре с ответчиком она указала свой контактный номер телефона.

Звонки на телефон стали поступать все чаще, представители ООО МКК «Конга» звонят в любое время суток, в том числе ночное время. Во время разговоров сотрудники ответчика разговаривают грубо, допускают хамские

выражения, угрожают начать звонить ей на работу и разглашать о ней порочащие сведения.

Она не давала согласие на использование ее персональных данных ответчиком. Однако, ее персональные данные, включая номер телефона, место работы, СНИЛС, контакты родственников незаконно хранятся и используются сотрудниками ответчика.

В индивидуальных условиях указан контактный номер (номер изъят), который ей не знаком и ей не принадлежит. И именно с этого номера она якобы подтвердила ее электронную почту. При этом договор заключен в 5-26 ч., т.е. во время в которое она еще спит. Также в документах ответчик указана электронная почта, которая ей никогда не принадлежала, не была известна и ею не регистрировалась.

В связи со сложившейся обстановкой и психологическим давлением со стороны сотрудников ООО МКК «КОНГА» у истца резко ухудшилось здоровье, она стала очень плохо спать, нервничать, боится находиться на улице, тем более, что требования сотрудников ответчика незаконны. Более того, сложившаяся ситуация негативно сказывается не только лично на ней, но и на ее семье. В связи с этим, компенсацию причиненного морального вреда истец оценивает в 300 000 руб.

В связи с тем, что самостоятельные попытки урегулировать ситуацию не привели к положительному результату, учитывая отсутствие у нее юридического образования, истец вынуждена была обратиться за правовой помощью, стоимость услуг составила 40 000 руб.

Истец просила суд взыскать с ООО МКК «КОНГА» в ее пользу денежную компенсацию морального вреда в размере 300 000 руб., судебные расходы в размере 40 000 руб., обязать ООО МКК «КОНГА» в кратчайшие сроки убрать из ее кредитной истории свои записи.

Решением Октябрьского районного суда города Иркутска от 5 февраля 2018 года в удовлетворении исковых требований отказано.

В апелляционной жалобе Варламова Е.В. ставит вопрос об отмене решения суда, считая его незаконным и необоснованным.

В обоснование своего несогласия с решением суда указывает, что ответчиком не предоставлены доказательства заключения кредитного договора с истцом, на кредитном договоре нет подписи истца, электронно-цифровой подписью она не пользуется. Об имеющихся претензиях со стороны ООО МКК «КОНГА» она узнала только из телефонных звонков.

Повторяет доводы иска о том, что из-за неправомерных действий ответчика и оказания на нее психологического давления у нее и ее семьи ухудшилось здоровье, они понесли нравственные страдания.

Полагает, что суд формально отнесся к рассмотрению дела, принял сторону ответчика, не дал правовой оценки приведенным истцом обстоятельствам и представленным в их обоснование доказательствам, чем нарушил нормы материального и процессуального права.

Возражений относительно апелляционной жалобы не поступило.

Судебная коллегия на основании статьи 167 Гражданского процессуального кодекса Российской Федерации (далее - ГПК РФ) рассмотрела дело в отсутствие неявившихся лиц, надлежащим образом извещенных о времени и месте судебного заседания, сведений об уважительности причин своей неявки не представивших, с заявлением о рассмотрении дела в свое отсутствие не обращавшихся.

Заслушав доклад по делу, изучив материалы дела, обсудив доводы апелляционной жалобы, проверив правильность применения судом норм материального и процессуального права, а также законность и обоснованность решения суда первой инстанции суд апелляционной инстанции приходит к следующим выводам.

Конституцией Российской Федерации к основным правам человека и гражданина отнесены достоинство личности (часть 1 статьи 21), а также неприкосновенность частной жизни (часть 1 статьи 23).

На основании п. 2 ст. 3 Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных" (далее Закон о персональных данных), оператором персональных данных признается государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Согласно ч. 3 ст. 6 Закона о персональных данных, оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора.

В соответствии с п. 5 ч. 1 вышеуказанной статьи, предусмотрено, что обработка персональных данных допускается в случае, если обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

В силу ч. 4 ст. 6 Закона о персональных данных, лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

Согласно ст. 151 Гражданского кодекса Российской Федерации (далее ГК РФ), если гражданину причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда.

Как было установлено судом первой инстанции и подтверждается материалами дела, ООО МКК «КОНГА» является действующим юридическим лицом, осуществляющим микрофинансовую деятельность.

Как усматривается из представленных ответчиком документов, истцом Варламовой Е.В. через сайт ООО МКК «КОНГА» (дата изъята) , с помощью сотрудника цента поддержки клиентов и андейррайтинга Тропининой Е.А., была заполнена анкета для получения микрозайма. В анкете Варламовой Е.В. указаны реквизиты паспорта, адрес места жительства, СНИЛС, номера телефонов – (номер изъят), (номер изъят), (номер изъят), (номер изъят), (номер изъят), (номер изъят), (номер изъят), (номер изъят), (номер изъят), электронный адрес (данные изъяты).

В дальнейшем ей были направлены Индивидуальные условия договора потребительского кредита (займа) № (номер изъят) от 22.08.2017, которые были подписаны электронной подписью заемщика.

Также к индивидуальным условиям приложено согласие Варламовой Е.В. на получение кредитного отчета, в котором она выразила согласие ООО МКК «КОНГА» на получение ее кредитного отчета, сформированного на основании ее кредитной истории в

Бюро (ООО «Эквифакс Кредит Сервисиз») с целью проверки благонадежности/выдачи займа. Выразила свое согласие на обработку ее персональных данных. При этом согласие на обработку персональных данных выдано до полного исполнения договора. Данное согласие также подписано электронной подписью.

Согласно информации о платеже, для исполнения условий договора, Варламовой Е.В. на счет № (номер изъят) ООО МКК «КОНГА» были перечислены денежные средства по договору займа № (номер изъят) от 22.08.2017 в сумме 2 000 руб. При этом факт перечисления денежных средств в 05-26 ч. не свидетельствует о необходимости обязательного непосредственного нахождения истца в этот период времени на сайте ООО МКК «КОНГА».

Согласно Индивидуальным условиям у Варламовой Е.В. возникла обязанность по возврату заемных денежных средств и начисленных процентов в размере 2 610,4 руб. в срок до 06.09.2017.

Обязательства по возврату денежных средств до настоящего времени не исполнены, задолженность по договору займа № (номер изъят) от 22.08.2017 не выплачена.Сведения о заемщике были переданы в Бюро кредитных историй, которыми подтверждается, что у Варламовой Е.В. имеется просроченная задолженность перед ООО МКК «КОНГА» в размере 3 720 руб.

Из установленных по делу обстоятельств, следует, что от имени Варламовой Е.В. через сайт ООО МКК «КОНГА» поступила заявка на получение кредита, с указанием всех ее персональных данных – фамилии, имени, отчества, паспортных данных, данных СНИЛС, адреса регистрации и проживания, контактных телефонов. С контактного телефона в ООО МКК «КОНГА» поступило подтверждение обращения за займом. Также ООО МКК «КОНГА» была предоставлена информация о счете, на которые подлежали перечислению кредитные средства. Вся информация проверялась ответчиком в соответствии с порядком, определенном в Правилах. Об отсутствии указанного заявителем счета сведения из банка при проверке не поступали, денежные средства были перечислены.

Оценив все представленные доказательства в их совокупности, и отказывая в удовлетворении исковых требований, руководствуясь положениями ст. ст. 151, 1101 ГК РФ, ст. ст. 6, 9, 17, 24 ФЗ "О персональных данных", ст. ст. 98, 100 ГПК РФ, суд пришел к выводу о том, что достоверных и допустимых доказательств нарушения прав истца ответчиком, суду первой инстанции истцом, в силу положений ч. 1 ст. 56 ГПК РФ, не было представлено, в связи с чем, суд обоснованно отказал в удовлетворении требований истца в полном объеме, поскольку доказательств злоупотребления ответчиком правом при телефонном взаимодействии с истцом, а равно совершения им действий, направленных на причинение истцу вреда, нравственных либо физических страданий не представлено.

При этом суд дал оценку индивидуальным условиям договора потребительского кредита (займа) от 22.08.2017, согласию Варламовой Е.В. на получение кредитного отчета и иным представленным ответчиком доказательствам, и пришел к выводу о том, что они не подтверждают наличие между истцом и ответчиком отношений по договору займа.

Судебная коллегия с указанными выводами суда первой инстанции полагает возможным согласиться в силу их законности и обоснованности. Ответчик как заимодавец не был лишен права в целях устранения просрочки исполнения обязательств по кредитному договору информировать заемщика о возможных последствиях.

В апелляционной жалобе приводятся доводы о том, что ответчик допустил незаконные действия по отношению к истице, выразившиеся в виде телефонных звонков, смс - сообщений с требованиями оплатить несуществующую задолженность по кредиту, с

угрозами. Указанные действия причинили истице и ее семье нравственные и физические страдания, они переживали, терпели неудобства, болели.

Согласно разъяснений, содержащихся в п. 1 постановления Пленума Верховного Суда Российской Федерации № 10 от 20.12.1994 г. "Некоторые вопросы применения законодательства о компенсации морального вреда", суду следует также устанавливать, чем подтверждается факт причинения потерпевшему нравственных или физических страданий, при каких обстоятельствах и какими действиями (бездействием) они нанесены, степень вины причинителя, какие нравственные или физические страдания перенесены потерпевшим, в какой сумме он оценивает их компенсацию и другие обстоятельства, имеющие значение для разрешения конкретного спора.

В силу п. 2 указанного Постановления под моральным вредом понимаются нравственные или физические страдания, причиненные действиями (бездействием), посягающими на принадлежащие гражданину от рождения или в силу закона нематериальные блага (жизнь, здоровье, достоинство личности, деловая репутация, неприкосновенность частной жизни, личная и семейная тайны и т.п.), или нарушающими его личные неимущественные права (право на пользование своим именем, право авторства и другие неимущественные права в соответствии с законами об охране прав на результаты интеллектуальной деятельности) либо нарушающими имущественные права гражданина.

Моральный вред, в частности, может заключаться в нравственных переживаниях в связи с тратой родственников, невозможностью продолжать активную общественную жизнь, потерей работы, раскрытием семейной, врачебной тайны, распространением не соответствующих действительности сведений, порочащих честь, достоинство или деловую репутацию гражданина, временным ограничением или лишением каких-либо прав, физической болью, связанной с причиненным увечьем, иным повреждением здоровья либо в связи с заболеванием, перенесенным в результате нравственных страданий и др.

Пункт 3 указанного Постановления содержит разъяснения о том, что в соответствии с действующим законодательством одним из обязательных условий наступления ответственности за причинение морального вреда является вина причинителя. Исключение составляют случаи, прямо предусмотренные законом. Например, когда: вред причинен жизни или здоровью гражданина источником повышенной опасности; вред причинен гражданину в результате его незаконного осуждения, незаконного применения в качестве меры пресечения заключения под стражу или подписки о невыезде, незаконного наложения административного взыскания в виде ареста или исправительных работ; вред причинен распространением сведений, порочащих честь, достоинство и деловую репутацию (ст. 1100 ГК РФ).

Каждая сторона должна доказать те обстоятельства, на которые она ссылается как на основания своих требований и возражений (ст. 56 ГПК РФ).

В данном случае допустимых доказательств, с достоверностью подтверждающих факт незаконных действий ответчика, приведших к причинению истице или ее семье нравственных и физических страданий, вызвавших ухудшение состояния здоровья, иные негативные последствия, ни в ходе судебного разбирательства, ни в суд апелляционной инстанции представлено не было, в связи с чем, соответствующие доводы апелляционной жалобы подлежат отклонению судебной коллегией.

Доводы апелляционной жалобы о том, что судом дана ненадлежащая оценка представленным по делу доказательствам, судебная коллегия отклоняет, поскольку, в силу положений ст. ст. 56, 59, 67 ГПК РФ, суд самостоятельно определяет какие обстоятельства имеют значение для дела, какой стороне их надлежит доказывать, принимает те доказательства, которые имеют значение для рассмотрения и разрешения дела, оценивает

доказательства по своему внутреннему убеждению, основанному на всестороннем, полном, объективном и непосредственном исследовании имеющихся в деле доказательств. Никакие доказательства не имеют для суда заранее установленной силы. Суд дал всем представленным сторонами доказательствам надлежащую правовую оценку, оснований не согласиться с которой у коллегии не имеется.

Проверив доводы апелляционной жалобы, судебная коллегия считает, что они не могут быть положены в основу отмены по существу правильного судебного постановления, так как сводятся к изложению обстоятельств, являвшихся предметом подробного исследования и оценки суда первой инстанции и к выражению несогласия с произведенной судом первой инстанции оценкой обстоятельств дела и представленных по делу доказательств, произведенной судом первой инстанции в полном соответствии с положениями статьи 67 ГПК РФ, тогда как оснований для иной оценки имеющихся в материалах дела доказательств суд апелляционной инстанции не усматривает.

При этом нарушений норм материального и процессуального права, повлекших вынесение незаконного решения, судом первой инстанции при рассмотрении настоящего дела не допущено.

Руководствуясь статьей 328 Гражданского процессуального кодекса Российской Федерации, судебная коллегия

О П Р Е Д Е Л И Л А:

решение Октябрьского районного суда города Иркутска от 5 февраля 2018 года по данному гражданскому делу оставить без изменения, апелляционную жалобу - без удовлетворения.

Судья-председательствующий Л.С. Гуревская

- **Дело №2-1183/2017**

Р Е Ш Е Н И Е

Именем Российской Федерации

г. Выкса 20 декабря 2017 г.

Выксунский городской суд Нижегородской области в составе председательствующего судьи Красовской Ю.О., при секретаре Бистерфельд С.А., с участием ответчика Смольянинова Ю.Г., рассмотрев в открытом судебном заседании гражданское дело по иску

Общества с ограниченной ответственностью «Русфинанс банк» к Смольянинову Ю. Г. о взыскании задолженности по кредитному договору,

по встречному иску

Смольянинова Ю. Г. к Обществу с ограниченной ответственностью «Русфинанс банк» о признании недействительным условий кредитного договора,

УСТАНОВИЛ

Общество с ограниченной ответственностью «Русфинанс банк» (далее ООО «Русфинанс банк», Банк или кредитор) обратилось в суд с иском к Смольянинову Ю.Г. о взыскании задолженности по Договору потребительского кредита №… от ДАТА в размере 190 371 руб. 83 коп., а также расходов по оплате государственной пошлины.

Исковые требования мотивированы тем, что между сторонами ДАТА был заключен Договор потребительского кредита №… на сумму 235 720 руб. 00 коп. Выдача кредита произведена путем перечисления денежных средств со счета заемщика на банковский счет торговой организации в оплату приобретаемого заемщиком товара. Таким образом, Общество с ограниченной ответственностью «Русфинанс банк» свои обязательства по выдаче кредита выполнило в полном объеме. Заемщик обязался исполнять обязанности по возврату кредита и уплате процентов в соответствии с графиком. Однако обязательства по своевременному возврату кредита и погашению начисленных процентов заемщик не выполняет, неоднократно допускал просрочки платежей. За период с ДАТА (дата образования просрочки) по ДАТА(дата составления расчета) по договору образовалась задолженность в размере 190371руб. 83коп., которая состоит из: текущего долга покредиту – 63234руб. 50коп., срочных процентов на сумму текущего долга – 5917руб. 99коп., просроченного кредита – 121219руб. 34коп.

Ответчик Смольянинов Ю.Г. обратился в суд со встречным иском к ООО «Русфинанс банк» о признании недействительными условия Договора потребительского кредита № … от ДАТА., заключенного между Смольяниновым Ю. Г. и Обществом с ограниченной ответственностью «Русфинанс банк», взыскании денежных средств в размере 75284руб. 88коп., а также судебных расходов.

Встречные исковые требования мотивированы тем, что кредитный договор с ООО «Русфинанс банк» он не заключал, заявление о выдачекредита и договор не подписывал, кредит не получал , в офисе банка не был, подпись клиента, поставленная в документах, не соответствует его подписи. Согласно Договору потребительского кредита №…. от ДАТА, цель использования клиентом потребительскогокредита – оплата стоимости приобретаемой мебели, где в п.22 индивидуальных условий договора продавцом товара указана … А.А., которая является … и могла иметь доступ к его данным. Менеджер, выдавший кредит , работала непосредственно в торговой точке А.А. Предполагает, что А.А., заручившись поддержкой недобросовестного кредитного менеджера, оформила кредит на покупку дорогостоящей мебели без его участия, начиная с ДАТА самостоятельно осуществляла платежи по кредиту , а позже, когда у неё возникли финансовые трудности прекратила вносить платежи, что и послужило поводом для банка обратиться в суд за взысканием долга. ДАТА в отношении него мировым судьей судебного участка № 2 Выксунского судебного района в пользу ООО «Русфинанс банк» взыскана задолженность по Договору потребительского кредита №… в сумме 263199руб. 53коп. и расходы по оплате государственной пошлины в размере 2916руб. Определением мирового судьи от.. .2017 по его заявлению указанный судебный приказ был отменен. Однако к этому времени в пользу ООО «Русфинанс банк» с него уже было взыскано 75284руб. 88коп. ДАТА он обратился в суд с заявлением о повороте исполнения вышеуказанного судебного приказа. Определением от ….2017 его заявление было удовлетворено, произведен поворот исполнения судебного приказа от …2017, исполнительное производство в отношении него прекращено. Однако в.. . 2017 ООО «Русфинанс банк» направило в суд исковое заявление о взыскании с него оставшейся суммы долга по кредитному договору.

Определением Выксунского городского суда от ….2017 исковые требования объединены в одно производство для совместного рассмотрения.

Определением Выксунского городского суда от.. .2017 производство по делу по встречному исковому заявлению Смольянинова Ю.Г. к ООО «Русфинанс банк» в части исковых требований о взыскании денежных средств в размере 75284руб. 88коп. прекращено в связи с отказом истца от иска в этой части.

В судебное заседание представитель истца ООО «Русфинанс Банк» не явился, ходатайствует о рассмотрении дела в отсутствие его представителя.

Ответчик Смольянинов Ю.Г. в судебном заседании исковые требования ООО «Русфинанс банк» не признал, заявленные им встречные требования поддержал, просил удовлетворить, указав, что условия Договора потребительского кредита №… от ДАТА являются недействительными, поскольку данный договор им не заключался и не подписывался, в связи с чем оснований для взыскания с него задолженности по данному договору не имеется. Одновременно просит взыскать с ООО «Русфинанс банк» понесенные им расходы по оплате за производство судебной почерковедческой экспертизы в размере 15450руб.

Исследовав и оценив собранные по делу доказательства в их совокупности в соответствии со ст.ст.12, 55, 56, 57, 59, 60, 67 ГПК РФ, установив юридически значимые обстоятельства по делу, суд находит следующее.

В силу ст.56 ГПК РФ каждая сторона обязана доказать те обстоятельства, на которые она ссылается как на обоснование своих требований или возражений. Бремя доказывания между сторонами распределено. Согласно ч.3 ст.196 ГПК РФ суд принимает решение по заявленным истцом требованиям.

Согласно ст. 9 ФЗ №15-ФЗ от 26.01.1996 г. "О введении в действие части второй Гражданского кодекса РФ", п.1 ст.1 Закона РФ "О защите прав потребителей", отношения с участием потребителей регулируются ГК РФ, Законом о защите прав потребителей, другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами РФ.

В соответствии со ст. 16 Закона «О защите прав потребителей», условия договора, ущемляющие права потребителя по сравнению с правилами, установленными законами или иными правовыми актами Российской Федерации в области защиты прав потребителей, признаются недействительными. При этом запрещается обуславливать приобретение одних услуг обязательным приобретением иных услуг. Убытки, причиненные потребителю вследствие нарушения его права на свободный выбор в данном случае, возмещаются исполнителем в полном объеме.

Частью 1 статьи 420 ГК РФ договором признается соглашение двух или нескольких лиц об установлении, изменении или прекращении гражданских прав и обязанностей.

В соответствии с п. 1 ст. 432 ГК РФ договор считается заключенным, если между сторонами, в требуемой в подлежащих случаях форме, достигнуто соглашение по всем существенным условиям договора.

Существенными являются условия о предмете договора, условия, которые названы в законе или иных правовых актах как существенные или необходимые для договоров данного вида, а также все те условия, относительно которых по заявлению одной из сторон должно быть достигнуто соглашение.

Из содержания ч. 2 ст. 434 ГК РФ следует, что договор в письменной форме может быть заключен путем составления одного документа, подписанного сторонами, а также путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору.

Согласно ст. 30 Закона РФ от 02.12.1990 "О банках и банковской деятельности" отношения между кредитными организациями и их клиентами осуществляются на основе договоров, если иное не установлено федеральным законом. В соответствии с настоящим Законом в договоре должны быть указаны процентные ставки по кредитам , стоимость банковских услуг и сроки их выполнения, имущественная ответственность сторон за нарушение договора, а также порядок расторжения договора и иные существенные условия договора. Клиенты вправе открывать необходимое им количество расчетных и иных счетов.

Судом по делу установлено, что ДАТА года между ООО «Русфинанс банк» (Кредитор) и Смольяниновым Ю. Г. (Заемщик) был заключен Договор потребительского кредита №…, согласно которому Кредитор обязался предоставить Заемщику кредит в размере 235 720 рублей (п.1) сроком до ДАТА под …% годовых.

Согласно п.11 Договора потребительского кредита №… от ДАТА, цель использования клиентом потребительского кредита – приобретение мебели: диван Ланкастер 99990руб., мебель группы А кресла кожаные Изобелла 48000руб., спальный гарнитур Изобелла 124000руб., общей стоимостью 271990руб., первоначальный взнос 36990руб., сумма кредита на товар – 235000руб.

Как следует из положений пунктов 21 и 22 Договора потребительского кредита №… от ДАТА, кредитор открывает счет № …, заемщик уполномочивает кредитора на списание с указанного счета денежных средств в размере суммы кредита , указанной в п.1 для дальнейшего перечисления на счет фирме - продавец товара … А.А. (… область, г. …, ул. … д…..

Договор потребительского кредита №… от ДАТА подписан клиентом с указанием расшифровки подписи – Смольянинов Ю. Г. Одновременно подписи клиента имеются на заявлении о предоставлении кредита и графике платежей, в соответствии с которым ежемесячный платеж по кредиту составил 13918руб., последний платеж в срок до ДАТА в размере 13515руб. 30коп.

Согласно выписки по лицевому счету № … с ДАТА по ДАТА обязательства по Договору потребительского кредита №… от ДАТА исполнялись заемщиком до ДАТА, после чего по договору стала образовываться просрочка, платежи заемщиком в счет погашения задолженности не вносились. По состоянию на ДАТА общая сумма задолженности по договору составила 190371руб. 83коп., из которых: текущий долг по кредиту – 63234руб. 50коп., срочные проценты на сумму текущего долга – 5917руб. 99коп., просроченный кредит – 121219руб. 34коп. Сумма долга подтверждена расчетом задолженности, представленным ООО «Русфинанс банк».

Наличие задолженности по Договору потребительского кредита №… от ДАТА послужило основанием для обращения истца с заявлением о вынесении судебного приказа по взысканию просроченного долга.

ДАТА на основании заявления ООО «Русфинанс банк» мировым судьей судебного участка № 2 Выксунского судебного района вынесен судебный приказ о взыскании со Смольянинова Ю.Г. в пользу ООО «Русфинанс банк» задолженности по Договору потребительскогокредита №…, который определением мирового судьи от ДАТА по заявлению Смольянинова Ю.Г. был отменен, в связи с чем ООО «Русфинанс банк» обратился в суд с настоящим иском.

В обосновании своих доводов ответчиком указывается на то обстоятельство, что кредитный договор с ООО «Русфинанс банк» он не заключал, заявление о выдаче кредита и договор не подписывал, кредит не получал , в офисе банка не был, подпись клиента, поставленная в документах, не соответствует его подписи.

Согласно ст.166 ГК РФ: Сделка недействительна по основаниям, установленным настоящим Кодексом, в силу признания ее таковой судом (оспоримая сделка) либо независимо от такого признания (ничтожная сделка). Требование о признании оспоримой сделки недействительной может быть предъявлено стороной сделки или иным лицом, указанным в законе. Оспоримая сделка может быть признана недействительной, если она нарушает права или охраняемые законом интересы лица, оспаривающего сделку, в том числе повлекла неблагоприятные для него последствия. В случаях, когда в соответствии с законом сделка оспаривается в интересах третьих лиц, она может быть признана недействительной, если нарушает права или охраняемые законом интересы таких третьих лиц.

В силу ст. 167 ГК РФ недействительная сделка не влечет юридических последствий, за исключением тех, которые связаны с ее недействительностью, и недействительна с момента ее совершения.

Статья 168 ГК РФ предусматривает, что за исключением случаев, предусмотренных пунктом 2 настоящей статьи или иным законом, сделка, нарушающая требования закона или иного правового акта, является оспоримой, если из закона не следует, что должны применяться другие последствия нарушения, не связанные с недействительностью сделки. Сделка, нарушающая требования закона или иного правового акта и при этом посягающая на публичные интересы либо права и охраняемые законом интересы третьих лиц, ничтожна, если из закона не следует, что такая сделка оспорима или должны применяться другие последствия нарушения, не связанные с недействительностью сделки.

Определением Выксунского городского суда Нижегородской области от … 2017 по ходатайству ответчика и истца по встречному иску Смольянинова Ю.Г. по делу назначена судебная почерковедческая экспертиза, проведение которой поручено экспертам ФГБУ «Приволжского регионального центра судебной экспертизы Министерства юстиции РФ», на разрешение эксперта поставлен вопрос: кому принадлежат Смольянинову Ю. Г. или иному лицу подписи, сделанные от имени Смольянинова Ю. Г. на следующих документах: Заявлении о предоставлении кредита от ДАТА, Договоре потребительского кредита №… от ДАТА, графике платежей от ДАТА?

Согласно заключению эксперта № … от ДАТА., подписи от имени Смольянинова Ю.Г., расположенные в печатной строке между печатной записью «Подпись клиента» и рукописной записью «Смольянинов Ю.Г.» в левом нижнем углу заявления Смольянинова Ю. Г в ООО «Русфинанс банк» о предоставлении кредита в сумме 235720,00 руб., номер

заявления ….от ДАТА; в печатной строке «подпись» между печатной записью «ФИО клиента» и рукописной записью «Смольянинов Ю. Г.» в первой строке ниже печатного текста на 4-й странице Договора потребительского кредита №… дата ДАТА, заключенного между ООО «Русфинанс банк» (Кредитор) с одной стороны и Смольяниновым Ю. Г. (Клиент) с другой стороны на сумму кредита 235720,00руб.; в печатной строке «подпись» между печатной записью «С Графиком платежей ознакомлен (а)» и рукописной записью «Смольянинов Ю.Г.» ниже печатного текста на каждой из 3-х страниц Графика платежей по кредитному договору №… Смольянинова Ю. Г. на сумму 235720,00руб. выполнены одним лицом – не самим Смольяниновым Ю. Г., а другим лицом с подражанием каким-то подлинным подписям Смольянинова Ю.Г.

Экспертное заключение было составлено в порядке ст.ст. 79,86 ГПК РФ.

Выводы эксперта основаны на материалах дела, научно обоснованы и соответствуют исследовательской части заключения, экспертом изучены и оценены все представленные доказательства. Эксперт предупрежден об уголовной ответственности за дачу заведомо ложного заключения и не является лицом, заинтересованным в исходе дела, в связи чем, суд полагает необходимым принять указанное экспертное заключение в качестве доказательства по делу.

Согласно п. 2 ст. 1 ГК РФ граждане и юридические лица приобретают и осуществляют свои гражданские права своей волей и в своем интересе. Они свободны в установлении своих прав и обязанностей на основе договора и определении любых, не противоречащих законодательству условий договора.

Согласно ст. 421 ГК РФ граждане и юридические лица свободны в заключении договора.

В соответствии со ст. 153 ГК РФ, сделками признаются действия граждан и юридических лиц, направленные на установление, изменение или прекращение гражданских прав и обязанностей.

В силу ч. 3 ст. 154 ГК РФ, для заключения договора необходимо выражение согласованной воли двух сторон (двусторонняя сделка) либо трех или более сторон (многосторонняя сделка).

Частью 1 ст. 420 ГК РФ договором признается соглашение двух или нескольких лиц об установлении, изменении или прекращении гражданских прав и обязанностей.

В силу ст. 820 ГК РФ, кредитный договор должен быть заключен в письменной форме.

Из содержания ч. 2 ст. 434 ГК РФ следует, что договор в письменной форме может быть заключен путем составления одного документа, подписанного сторонами, а также путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору.

В соответствии с ч. 1 ст. 807 ГК РФ договор займа считается заключенным с момента передачи денег или других вещей.

В силу системного толкования ст. ст. 309, 421, 820 ГК РФ подписание договора стороной свидетельствует о выражении его воли на принятие соответствующего обязательства.

Положения Гражданского кодекса Российской Федерации, законов и иных актов, содержащих нормы гражданского права (ст. 3 ГК РФ), подлежат истолкованию в системной взаимосвязи с основными началами гражданского законодательства, закрепленными а статье 1 ГК РФ.

В соответствии с п. 3 ст. 1 ГК РФ при установлении, осуществлении и защите гражданских прав и при исполнении гражданских обязанностей участники гражданских правоотношений должны действовать добросовестно.

В силу п. 4 ст. 1 ГК РФ, никто не вправе извлекать преимущество из своего незаконного или недобросовестного поведения.

По общему правилу п. 5 ст. 10 ГК РФ добросовестность участников гражданских правоотношений и разумность их действий предполагаются, пока не доказано иное.

Согласно ст. 168 ГК РФ сделка, не соответствующая требованиям закона или иных правовых актов, ничтожна, если закон не устанавливает, что такая сделка оспорима, или не предусматривает иных последствий нарушения.

Наличие в договоре поддельной подписи одного из его участников свидетельствует о ничтожности договора как сфальсифицированного документа согласно ст. 168 ГК РФ независимо от признания его таковым судом.

Исходя из установленных по делу обстоятельств, с учетом указанного заключения судебной почерковедческой экспертизы, основываясь на положениях вышеназванных правовых норм, суд приходит к выводу о том, что истец по встречному иску Смольянинов Ю.Г. Договор потребительского кредита №…. от ДАТА не подписывал, следовательно, не согласовывал с Банком его существенные условия.

При таких обстоятельствах условия договора не могут считаться согласованными, а договор заключенным. Письменная форма договора не соблюдена, каких-либо юридических последствий он не порождает.

С учетом вышеизложенного, при установленных судом обстоятельствах, исковые требования истца по встречному иску Смольянинова Ю.Г. о признании недействительными условия Договора потребительского кредита № … от ДАТА., заключенного между Смольяниновым Ю. Г. и Обществом с ограниченной ответственностью «Русфинанс банк», подлежат удовлетворению. При этом оснований для взыскания со Смольянинова Ю.Г. задолженности по указанному договору в размере 190371,83руб. не имеется с учетом недействительности данного договора, в связи с чем в удовлетворении исковых требований ООО «Русфинанс банк» следует отказать.

Согласно ст.88 ГПК РФ судебные расходы состоят из государственной пошлины и издержек, связанных с рассмотрением дела.

В соответствии со ст.94 ГПК РФ: к издержкам, связанным с рассмотрением дела, относятся: суммы, подлежащие выплате свидетелям, экспертам, специалистам и переводчикам; расходы на оплату услуг переводчика, понесенные иностранными

гражданами и лицами без гражданства, если иное не предусмотрено международным договором Российской Федерации; расходы на проезд и проживание сторон и третьих лиц, понесенные ими в связи с явкой в суд; расходы на оплату услуг представителей; расходы на производство осмотра на месте; компенсация за фактическую потерю времени в соответствии со ст.90 ГПК РФ; связанные с рассмотрением дела почтовые расходы, понесенные сторонами; другие признанные судом необходимыми расходы.

Согласно ст. 98 ГПК РФ, стороне, в пользу которой состоялось решение суда, суд присуждает возместить с другой стороны все понесенные по делу судебные расходы, за исключением случаев, предусмотренных частью второй ст. 96 ГПК РФ.

Оплата за проведение экспертизы, назначенной судом по ходатайству ответчика (истца по встречному иску), определением суда от ДАТА г. была возложена на Смольянинова Ю.Г. Оплата за экспертизу произведена в полном объеме в размере 15450руб. Поскольку требования истца по встречному иску судом признаны обоснованными, с ООО «Русфинанс банк» в пользу Смольянинова Ю.Г. подлежат взысканию расходы по оплате экспертизы в размере 15000руб., а также комиссия банка в сумме 450руб. за перевод денежных средств по квитанции от ДАТА.

На основании изложенного, руководствуясь ст.ст.194-199 ГПК РФ, суд

р е ш и л:

В удовлетворении исковых требований к Смольянинову Ю. Г. о взыскании задолженности по Договору потребительского кредита № …. от ДАТА. Обществу с ограниченной ответственностью «Русфинанс банк» отказать.

Встречные исковые требования Смольянинова Ю. Г. удовлетворить.

Признать недействительными условия Договора потребительского кредита № …. от ДАТА., заключенного между Смольяниновым Ю. Г. и Обществом с ограниченной ответственностью «Русфинанс банк» в силу ничтожности.

Взыскать с Общества с ограниченной ответственностью «Русфинанс банк» в пользу Смольянинова Ю. Г. расходы по оплате судебной экспертизы в размере 15450,00 рублей.

Решение может быть обжаловано в апелляционном порядке в Нижегородский областной суд путем подачи жалобы через Выксунский городской суд в течение месяца с момента изготовления мотивированного решения.

Судья-Красовская Ю.О.

Некоторые рекомендации адвокатов по оспариванию «чужого» кредита в суде:

- **Конструктор исковых заявлений и жалоб – Как оспорить в суде кредитный договор, оформленный по чужому паспорту? https://iskivsem.ru/faq/209**

«Как оспорить в суде кредитный договор, оформленный по чужому паспорту?

Кредитный договор может быть признан недействительным полностью или в части.

Недействительным признается кредитный договор, заключенный:

с нарушением требований закона или иных правовых актов (ст. 168 ГК РФ);

с целью, противной основам правопорядка и нравственности (ст. 169 ГК РФ);

недееспособным либо ограниченным судом в дееспособности лицом; лицом, не способным понимать значение своих действий или руководить ими, либо несовершеннолетним с нарушением установленного порядка, например без согласия родителей, усыновителей или попечителей (ст. ст. 171, 172, 175, 176, 177 ГК РФ);

под влиянием заблуждения (ст. 178 ГК РФ);

под влиянием обмана, насилия, угрозы или неблагоприятных обстоятельств (ст. 179 ГК РФ);

если кредитный договор является мнимой сделкой - совершенной без намерения создать соответствующие ему правовые последствия, или притворной сделкой - совершенной с целью прикрыть другую сделку (ст. 170 ГК РФ).

Если человек вдруг узнает от банка о том, что на его имя взят кредит и уже по нему существует задолженность, то в первую очередь ему необходимо отправить в банк письменное обращение о том, что лицо к кредиту не имеет никакого отношения. В этом же обращении необходимо попросить предоставить копию кредитного договора. Она понадобится как для обращения в милицию с заявлением о мошенничестве, так и в рамках возможных судебных разбирательств. Далее следует обратиться в полицию с заявлением по факту совершенного мошенничества и подделки документов. В заявлении необходимо сделать акцент на том, что подпись на кредитном договоре является фальшивой. Следует помнить, что часто к мошенничеству могут быть причастны и сотрудники банка, поскольку при выдаче кредита они обязаны удостовериться в личности заемщика, проверив не только его паспорт, но и другие документы. Кроме того, сейчас многие банки перед выдачей кредита фотографируют человека.

В случае если банк продолжает настаивать на оплате чужой задолженности, то рекомендуем как можно быстрее обратиться в суд с исковым заявлением о признании кредитного договора недействительным. В случае, когда банк уже обратился с иском о взыскании задолженности, то в этом случае следует обратиться в суд с встречным иском о признании кредитного договора недействительным (однако рекомендуется опередить банк в такой ситуации).

С учетом того что выяснение вопроса о том, принадлежит ли подпись в кредитном договоре и в иных документах, предлагаемых банком для подписания (анкетах заявления, карточке с образцами подписи, квитанции и др.), заемщику, относится к области специальных знаний, необходимо заявить ходатайство о назначении по делу почерковедческой экспертизы в порядке, предусмотренном ст. ст. 79 - 81 ГПК РФ. Если экспертным заключением будет четко и однозначно установлено, что заемщик кредитный договор не подписывал, а проставленная на данном документе подпись принадлежит иному лицу, то в удовлетворении иска банка о взыскании с него долга будет отказано в полном объеме. Так, в одном деле, отказывая банку в иске о взыскании с заемщика задолженности по кредиту, суд руководствовался ст. ст. 17, 21, 22, 154, 160, 166, 167, 168, 421, 432, 434, 819, 820 ГК РФ, согласно которым договор должен быть подписан сторонами, для заключения договора необходимо выражение согласованной воли сторон, при этом сделка, не соответствующая требованиям закона, ничтожна, недействительная сделка не влечет юридических последствий. Таким

образом, экспертное заключение в таком судебном деле является одним из самых весомых доказательств недействительности кредитного договора. Однако, если представленное в материалы дела экспертное заключение не будет содержать четкий и однозначный вывод о том, что заемщик спорный кредитный договор не подписывал, рассчитывать на освобождение от кредитного долга ему не следует, так как обязанность доказывания подделки подписи лежит на заемщике и при наличии заключения эксперта о невозможности определить подлинность подписи она не считается подложной. Таким образом, если бесспорных доказательств в пользу того, что заемщик не подписывал кредитного договора, нет, этот факт суд не может считать установленным.

Помимо результатов экспертизы, суду должны быть представлены такое доказательства как талон-уведомление, заявление заемщика в полицию с описанием всех обстоятельств произошедшего. Обращение в полицию по факту мошеннических действий, безусловно, необходимо, поскольку о совершенном преступлении надо заявить.

Дополнительно может быть представлено письмо территориального отдела ФМС России о том, что в период заключения кредитного договора заемщик обращался по факту утраты или хищения паспорта, за временным удостоверением личности и др. (см. Апелляционное определение Мосгорсуда от 16.02.2015 г. по делу N 33-0049).

Показания свидетелей также допустимы при рассмотрении таких требований.

Внимание: заемщиком может быть представлено доказательство отсутствия в городе заключения кредитного договора (например, командировочное удостоверение, проездной билет, судебное решение, вынесенное в другом городе с участием заемщика, судебная повестка с отметкой и т.д.)».

2.4. Мнения профессиональных участников рынка и экспертов

- **Forbes – Детектив о микрозаймах. Как вычислить мошенников в онлайне**
  http://www.forbes.ru/finansy-i-investicii/356475-detektiv-o-mikrozaymah-kak-vychislit-moshennikov-v-onlayne

«Борьба с мошенничеством в онлайн-кредитовании важна не только для самих микрофинансовых организаций, но и для добросовестных заемщиков – ведь от ее успеха во многом зависят условия по займам

У развития технологий, к сожалению, есть и обратная сторона: мошенники, которые ранее орудовали на рынках и улицах, теперь перешли в интернет. От их действий страдают в первую очередь сервисы, которые дают прямой доступ к деньгам: криптовалютные биржи, электронные кошельки, страховые компании и микрофинансовые организации.

Согласно статистике Webbankir, в среднем 5–6% поступающих заявок от потенциальных заемщиков имеют признаки мошенничества. Ситуация еще больше настораживает, если смотреть на первичные обращения. Здесь доля сомнительных заявок в разы выше. Иными словами, почти каждый третий клиент, который впервые обращается за займом, может действовать в мошеннических целях.

Конечно, риск дефолта существует всегда. Любой человек может неправильно оценить свои финансовые возможности, или возникнут внезапные обстоятельства, которые

помешают ему расплатиться в срок. Главное отличие мошенника в том, что он с самого начала не собирается возвращать деньги.

Факт мошенничества вскрывается, когда заемщик отказывается платить и сообщает, что не брал заем, а это сделал за него кто-то другой. Бывают случаи, когда мошенники берут займы на людей, которых хорошо знают, – соседей, родственников или знакомых. Или даже занимают друг на друга.

Как правило, суммы займов невелики – до 15 тысяч рублей. Однако профессиональные мошенники действуют с большим размахом, подавая десятки, сотни или даже тысячи заявок в различные микрофинансовые компании. В итоге отрасль и отдельные компании несут многомиллионные убытки. Причем чем крупнее бизнес, тем больше вероятность, что он станет мишенью мошенников.

Как работают мошенники

Основные виды мошенничества в онлайн-кредитовании – это получение займов на подставных лиц, подделка документов и получение сведений по кредитным историям незаконными способами. Во всех этих случаях необходим доступ к конфиденциальной информации (паспортные данные, ИНН, номера телефонов, места работы и т.п.). В ход идут нелегально добытые базы данных и фишинговые сайты, которые маскируются под ресурсы легальных организаций, чтобы заставить пользователя ввести нужные сведения.

За первые восемь месяцев 2017 года ФинЦЕРТ (структурное подразделение Банка России, отвечающее за мониторинг и реагирование на компьютерные атаки в кредитно-финансовой сфере) обнаружил 481 мошеннический домен различной тематики.

В топ-5 вошли сервисы p2p-переводов (84 домена), страховые компании (45), лжебанки (44), финансовые пирамиды (39) и лже-МФО (29). В ЦБ также сообщили о 309 жалобах клиентов микрофинансовых организаций на хищение персональных данных за этот период. Казалось бы, три сотни на всю Россию – цифра не слишком внушительная, но еще в 2016 году подобных жалоб не было зарегистрировано вовсе.

Оформив заем на другое лицо, мошенники-любители часто переводят деньги на собственную банковскую карту. В этом случае вычислить злоумышленника не составляет никакого труда. Более опытные мошенники используют так называемые «дропы» – банковские карты, открытые на чужое имя. Часто они выпускаются на бомжей: если у человека есть паспорт, многие банки откроют ему дебетовую карту.

Есть и люди, которые намеренно оформляют на себя карты, чтобы потом продать их третьим лицам и заявить о пропаже. К тому моменту, когда банк заблокирует карточку, мошенник уже успеет обналичить по ней средства.

Готовы ли МФО прощать

Популярность онлайн-кредитования у мошенников имеет под собой несколько причин. Прежде всего, это непростая экономическая ситуация, которая заставляет людей искать не совсем честные, а подчас и вовсе нелегальные способы заработка. Бытует распространенный миф, будто МФО готовы списать любые потери, ведь они все равно останутся в прибыли благодаря астрономическим процентам.

Отчасти эти настроения подогревают официальные лица, когда называют микрофинансовые компании «мироедами», «хуже старухи-процентщицы» и т.п. Украсть деньги нехорошо, а обмануть «мироеда» вроде как уже и нормально – ты почти Робин Гуд.

Для получения онлайн-займа не надо посещать офис, общаться с сотрудником кредитной организации и показывать паспорт. Интернет создает ощущение анонимности и безнаказанности. Именно поэтому здесь доля сомнительных заявок в разы выше, чем в традиционном кредитовании, где она не превышает 1%. Готовы ли компании, работающие в интернете, с этим мириться? На самом деле нет.

Процентные ставки в микрофинансировании действительно выше, чем в банковском потребительском кредитовании, но и дефолты допускаются в 2 раза чаще. Приемлемым уровнем считается, если не возвращаются 15–20% займов.

Высокие процентные ставки как раз и призваны компенсировать дефолтные риски. Поэтому вопреки распространенному мифу, любая попытка мошенничества, даже на 3 000 рублей, тщательно расследуется службой экономической безопасности. Ведь чем лучше компания умеет пресекать мошеннические действия, тем более выгодное предложение она может сделать для добропорядочных заемщиков.

Как вычислить мошенника

Борьба с мошенниками начинается еще на этапе рассмотрения заявки. Благодаря использованию больших данных сегодня узнать о человеке в интернете можно гораздо больше, чем при личном общении. Каждый заемщик анализируется по нескольким сотням различных параметров: кредитная история, проверка на соответствие паспортных и анкетных данных, профили в соцсетях и так далее. Ни один из признаков не позволяет однозначно заключить, что заявка подается мошенником, однако в совокупности они дают весьма ясную картину.

Вот некоторые подозрительные триггеры. Человек, впервые обратившийся в компанию, не интересуется условиями получения займа, то есть не изучает сайт и не пользуется кредитным калькулятором. При заполнении заявки он часто вводит данные с помощью копипаста, что указывает на наличие шаблона – скорее всего, человек подает заявки сразу во многие компании.

Он указывает в анкете, что живет и работает в одном городе, а по геотаргетингу находится сейчас в другом. Несколько заявок подаются с одного и того же IP или с похожих телефонных номеров (чтобы подать большое число заявок, мошенники часто скупают сим-карты оптом и номера отличаются одной–двумя цифрами). Учитывается и то, какие сайты посещал пользователь. Для этого используются так называемые evercookies – куки, которые невозможно удалить простой очисткой истории браузера.

Существенно повысить контроль угроз помогает сотрудничество с сотовыми операторами. Благодаря тому, что они отслеживают сигналы телефонов по вышкам сотовой связи, установить местонахождение человека можно даже в том случае, если он не разрешал доступ к своей геолокации. Кроме того, сотовые операторы знают IMEI – идентификационный номер каждого мобильного телефона, зарегистрированного в сети. Это позволяет отслеживать звонки не только с определенной сим-карты, но и с конкретного устройства. Мошенники часто пользуются разными сим-картами, а вот телефон меняют ради одного звонка далеко не все.

Из новых средств борьбы с мошенниками можно отметить появление антимошеннических сервисов на базе бюро кредитных историй. Они проходят сейчас этап тестирования. Принцип их действия похож на скоринговую модель – фактически они позволяют компаниям обмениваться данными о подозрительных клиентах и принимать решение о выдаче займа, основываясь не только на своей, но и на статистике других участников рынка. Мера обещает быть весьма эффективной, учитывая, что, как правило, мошенники делают веерные запросы в несколько различных МФО.

В свою очередь регулятор также постоянно внедряет новые системы идентификации, усложняющие жизнь мошенникам. Например, согласно закону «О кредитных историях», с 2017 года финансовые организации могут получать данные о кредитных историях граждан из БКИ только при наличии страхового номера индивидуального лицевого счета (СНИЛС).

Фактически это означает, что при оформлении заявки заемщик обязан указать свой СНИЛС. Поскольку это менее распространенная информация, чем паспортные данные, то на какое-то время количество мошенников действительно сократилось.

Сегодня Центробанк планирует распространить на финансовый рынок программу ЕСИА (Единую систему идентификации и аутентификации), которая уже обеспечивает санкционированный доступ граждан к сведениям, содержащимся в государственных информационных системах, через сайт госуслуг. Предполагается, что раз в год россияне будут приходить в уполномоченные пункты и по предъявлении паспорта получать уникальный код для проведения финансовых операций в интернете.

Ответственность за утерю кода будет нести сам человек, как, например, в случае с пин-кодом от банковской карты. То есть получить доступ к этой информации будет, по крайней мере, так же сложно, как и взломать банковскую карту.

Какова расплата

Если мошенничество все же произошло, задача службы экономической безопасности определить – действительно ли человек не брал деньги и стал жертвой злоумышленников или пытается таким образом отказаться выплачивать долг. Устанавливается, кто и когда оформлял заем, кто принимал решение о его выдаче, какие данные заемщика могут не соответствовать действительности.

Человек, на чье имя мошенники оформили заем, несет репутационные риски (испорченная кредитная история, звонки от коллекторов и так далее.). Однако прямой материальный ущерб несет именно компания, поэтому по факту проверки она обязательно подаст заявление в полицию.

Результатом, как правило, становятся реальные уголовные дела с ограничением свободы до двух лет и выплатами компенсаций в пользу государства. Так что получить судимость за кражу 10 000 рублей вполне реально. И совсем неумно».

- **Ведомости – Кредитные мошенники становятся все изобретательнее** **https://www.vedomosti.ru/finance/articles/2016/06/16/645506-kreditnie-moshenniki**

«А банки фиксируют рост числа «подозрительных» заявок на кредиты

В I квартале 2016 г. количество заявок, отмеченных банками как подозрительные, выросло на 82% по сравнению с аналогичным периодом прошлого года, при том что общее количество входящих заявлений увеличилось менее чем на 30%, следует из данных Объединенного бюро кредитных историй. Доля подозрительных заявок в общем потоке заявлений также выросла с 2,7 до 3,5%. Количество счетов, когда кредит уже выдан, но по нему нет первого платежа, что косвенно может свидетельствовать о кредитном мошенничестве, выросло на 40% до 267 106 счетов в I квартале этого года по сравнению с прошлым, свидетельствуют данные Национального бюро кредитных историй.

Растет уровень подготовки мошенников. «Сейчас мошенников сложно вычислить, даже тщательно проверив предоставляемые ими для получения кредита документы: они очень качественно их подделывают, вклеивают свои фотографии на документы других людей и прочее», – рассказывает представитель «Тинькофф банка». По его словам, определить, что документ поддельный, зачастую сложно даже с помощью специальной дорогостоящей техники.

«Мы видим в целом по системе, что есть тренд на рост мошенничества с кредитными заявками», – подтверждает директор департамента потребительского кредитования Русфинансбанка Александр Воронин. По его словам, самая распространенная мошенническая схема осуществляется с привлечением кредитного эксперта в магазине, который оформляет кредит на товар, используя подложные документы клиентов, или оформляет кредит на реальных клиентов, но находящихся в сговоре с перекупщиками товара. Как правило, указывает Воронин, такую схему мошенники используют в магазинах, где продаются товары, которые легко сбыть: мобильные телефоны или ноутбуки. Поэтому в такие магазины банки стараются направлять собственных сотрудников.

Одним из инструментов, с помощью которого банк определяет мошенников, является технология распознавания и сверки лиц по фотографии со встречи с сотрудником банка, говорит представитель «Тинькофф банка». И добавляет, что с начала года благодаря этому банк выявил 185 кредитных заявок, которые были поданы с представлением поддельных документов, ни одна из них не одобрена. «Мы помним случай, когда один и тот же человек по разным паспортам подал 10 заявок на кредит», – указывает он.

В «Тинькофф банке» скоринг по заявке осуществляется на всех этапах взаимодействия с клиентом. Банк анализирует полученную информацию и сопоставляет ее с имеющимся массивом данных, что позволяет эффективно выявлять мошенников, говорит представитель «Тинькофф банка».

В целом проверка при выдаче pos-кредитов проходит в три этапа, перечисляет Воронин: сначала сотрудник магазина или банка визуально оценивает клиента и его поведение, проверяет документы и заносит паспортные данные в анкету, делает фото или даже короткое видео клиента. Затем паспорт проверяется по базе ФМС, а информация о клиенте проверяется по базе кредитного бюро и проходит оценку скоринговой системы банка. На третьем этапе делается контрольный звонок клиенту в момент оформления кредита или спустя некоторое время. Если обнаружится подозрение на мошенничество, кредитный эксперт и магазин блокируются в системах банка, заключает он».

- **Экспрессденьги – Мошенники пытаются получать кредиты в интернете по чужим документам**

https://xn--c1abcbqhymjida0md.xn--p1ai/info/articles/moshenniki-pitayutsya-poluchat-krediti-v-internete-po-chuzhim-dokumentam/

«Для получения денег по подложным документам мошенники предпочитают обращаться в сервисы онлайн-кредитования, а не в традиционные кредитные организации. К таким результатам пришли эксперты из Объединенного кредитного бюро (ОКБ), оценив уровень сомнительных заявок, поданных на получение денег за последние два года.

Количество заявлений на получение денег, которые были признаны потенциально мошенническими, за 2016-2017 годы в банковской сфере уменьшилось вдвое и сейчас составляет 1,5% от общего числа обращений клиентов. За тот же срок в секторе онлайн-кредитования данный показатель увеличился почти до 6%. Чаще всего недобросовестные заемщики пытаются оформить заем или получить кредит по чужому паспорту.

По мнению экспертов, снижение числа рискованных заявок в традиционных кредитных учреждениях и их увеличение в онлайн-сегменте связано сразу с несколькими причинами. Во-первых, при дистанционном размещении заявки на получение денег мошенники меньше рискуют быть пойманными за руку. Во-вторых, среди людей укрепилось мнение, что специалисты сервисов по кредитованию в интернете уделяют меньше внимания предоставленным документам. Наконец, мошенники полагают, что микрофинансовые организации, предоставляющие услуги онлайн, применяют менее совершенные системы оценки кредитоспособности заявителя, или скоринга.

Несмотря на то, что потенциально мошенническими были признаны 6% заявлений, поданных в онлайн-сервисы кредитования, реальный процент пропущенных недостоверных заявлений за последний год оказался значительно меньше – всего 0,3%. Вопреки бытующему мнению, это связано с наиболее совершенными системами скоринга, которыми располагают участники рынка онлайн-кредитования. Их оснащение оказывается куда более совершенным, чем у банков, из-за специфики работы, когда сотрудник организации не имеет личного контакта с заемщиком.

Согласно статистике, больше всего подозрительных заявок на интернет-займы поступает из Ингушетии, Чечни, Дагестана и Кабардино-Балкарии. На эти северокавказские республики приходится более трети всех сомнительных обращений в онлайн-сервисы кредитования. От 5% до 5,5% подозрительных заявок на онлайн-займы поступает из таких российских регионов, как Красноярский край, Свердловская область и Республика Коми. В Санкт-Петербурге и Москве количество потенциально мошеннических заявлений, по данным ОКБ, составляет 1,7% и 1,5% соответственно».

- **Микрозаймы России – Как взять микрозайм на чужой паспорт?**
  https://mikrozajm.com/voprosy-i-otvety/kak-vzyat-mikrozajjm-na-chuzhojj-pasport/

«Как взять микрозайм на чужой паспорт?

Для того, чтобы взять микрозайм необходимо предоставить документы, которые удостоверяют вашу личность. Делается это специально для того, чтобы некое лицо не могло возложить финансовые обязательства на другого человека без его ведома, т.к. законодательство РФ квалифицирует данное действие как мошенничество.

Но такие ситуации все же происходят. В различных изданиях СМИ периодически освещаются ситуации, когда по чужому паспорту брали потребительские кредиты и экспресс займы и что потом доказать свою непричастность к этим событиям еще надо постараться.

Но многие компании, которые выдают займы через интернет и работают именно с копиями документов

Действительно, МФО выдающие подобные займы не имеют представительств, да и вообще не работают клиентом напрямую. Все операции проводятся исключительно дистанционным способом. Многие наверное сразу подумали, что оформить микрозайм на чужой паспорт онлайн через интернет получается вполне реально. А вот и нет!

- Если кредитные средства выплачиваются на кредитные карты, то их надо привязать в личном кабинете и они должны быть только именными. Это значит, что помимо чужих документов у мошенника должна быть еще карта. Но как правило владелец сразу же блокирует её после потери.
- Если деньги переводятся на электронные кошельки (яндекс.деньги, webmoney, qiwi и т.д.), то допускаются только их идентифицированные версии. Это значит, что их владелец предоставил все необходимые документы и подтвердил свою личность. А обычные кошельки и аккаунты никто не обслуживает.

Вот так на практике происходит взаимодействие между МФО и клиентом, поэтому всячески рекомендуем воздержаться от необдуманных действий в погоне за легкой наживой.

Еще раз о мерах личной безопасности для каждого

Порой пренебрежение простыми правилами может иметь большую цену для нас, но мы все равно надеемся на «авось». Помните, что знание и их применение совершенно разные вещи, поэтому прочтите еще раз, запомните и в случае чего, неукоснительно соблюдайте их.

- Если вы потеряли паспорт и после тщательных поисков так и не смогли его найти – пишите заявление о потери документов. Да, его восстановление повлечет множество неудобств и потерю времени, но лучше так.
- Бывают ситуации, когда действительно необходимо выслать скан паспорта. Рекомендуем воспользоваться графическим редактором и нанести диагональную полосу красного цвета и текст, что данный скан отправляется «тому-то» и с «такой-то» целью. Но делать это надо с полным пониманием всей ситуации.
- Никому и никогда не сообщайте срок годности и CVV код (последние три цифры на обратной стороне) ваше кредитной карты. Допускается только информирование о своем номере карты (12 цифр на лицевой стороне), если вы принимаете перевод.
- Если вы владелец интернет-кошельков и различных платежных систем, то регулярно меняйте пароль и пользуйтесь платными антивирусами. Задействуйте сложную авторизацию. Например для того, чтобы попасть в ваш аккаунт мало ввести правильный пароль, надо еще ввести содержание sms-сообщение, которое будет вам отправлено сервисом.

Как видите получить нелегально микрозайм очень сложно, но не давайте даже малейшего шанса злоумышленникам и тщательно оберегайте свои личные данные».

3. Кейс «P2P-кредитование»

Равноправное кредитование (также равноправное инвестирование или социальный заем; также краудлендинг; часто используется сокращение «заем P2P», (Peer-to-Peer) (англ.) – это способ ссуживания денег никоим образом не связанным между собой лицам или «равноправным сторонам» без привлечения традиционного финансового посредника, – например, банка или другого обычного финансового института. Займы предоставляются онлайн на вебсайтах специальных кредитных организаций посредством разнообразных платформ кредитования и инструментов проверки кредитоспособности. (Википедия).

При работе над этим кейсом обратите внимание на «терминологический разброс» при определении содержания отношений в этом сегменте финансового рынка, а также на содержательное разнообразие имеющихся сервисов и платформ.

3.1. Динамика P2P-кредитования

3.1.1. Мониторинг Банка России

Банк России проводит мониторинг рынка P2P кредитования с 2015 года.

- **Центральный банк Российской Федерации – Объем рынка краудфандинга в 2017 году увеличился в два раза http://www.cbr.ru/press/event/?id=1902**

«Объем рынка краудфандинга в 2017 году увеличился в два раза

Общий объем рынка краудфандинга в 2017 году составил 11,2 млрд рублей, что почти в два раза больше, чем в 2016 году (6,2 млрд рублей), и в 7,5 раза больше, чем в 2015 году (1,5 млрд рублей). Такие данные Банк России получил в результате мониторинга рынка краудфандинга, который проводится совместно с площадками, добровольно предоставляющими отчетность регулятору.

Сумма заключенных сделок P2P (выдача займов физическому лицу физическим лицом) выросла практически в два раза по сравнению с предыдущим периодом, достигнув 208,8 млн рублей. Средняя сумма одного договора займа в 2017 году составила 8915 рублей. Сохранилась тенденция к росту числа заемщиков (темп прироста – 129,1%), при этом на треть снизилось количество заимодавцев (34,9%).

P2B (выдача займов юридическому лицу или индивидуальному предпринимателю физическим лицом) – один из самых крупных и наиболее динамично развивающихся сегментов на рынке краудфандинга – в 2017 году показал устойчивый рост по всем оцениваемым показателям. Его объем достиг 1,55 млрд рублей, что на 216,3% больше, чем в 2016 году. Средняя сумма сделки в 2017 году составила практически 300 тыс. рублей на одного человека, средняя сумма займа – чуть более 900 тыс. рублей одному юридическому лицу. В свою очередь объем портфеля займов в данном сегменте составил 1,15 млрд рублей (что на 234% больше, чем в 2016 году). Доля просроченной задолженности в портфеле займов P2B снизилась на 0,9 п.п. по сравнению с 2016 годом (с 8,7 до 7,8%).

Резкий скачок произошел в объемах сегмента B2B (выдача займов юридическому лицу / индивидуальному предпринимателю юридическим лицом или индивидуальным предпринимателем), что было обусловлено присоединением к добровольной отчетности

новой компании, сразу занявшей место самого крупного игрока на рынке B2B (с долей в 83,4% совокупного портфеля займов). Таким образом, объем данного сегмента за 2017 год с учетом показателей крупнейшей площадки составил 9,3 млрд рублей, что на 81,5% больше, чем в 2016 году. В общей сложности в 2017 году было заключено 9442 B2B-договора.

В сегменте краудинвестинга (привлечение финансирования юридическим лицом в обмен на долю в уставном капитале, конвертируемые займы и т.д.), где инвесторами выступили в основном физические лица, произошло снижение объемов – до 153,2 млн рублей, что на 168,4 млн рублей (52,4%) меньше, чем в 2016 году. Всего в 2017 году при помощи краудинвестинговых площадок были привлечены инвестиции в 19 компаний. Средняя сумма, направленная на финансирование одного проекта, составила 8,1 млн рублей.

Краудфандинговый сектор Rewards (привлечение финансирования в проекты в обмен на нефинансовое вознаграждение) в 2017 году оставался традиционно стабильным. Было профинансировано 2,5 тыс. проектов, на реализацию которых привлечено почти 163 млн рублей. Средняя сумма, привлеченная на осуществление одного проекта, составила 53 036 рублей, а одного успешного проекта – 66 485 рублей.

Банк России проводит мониторинг рынка краудфандинга с 2015 года. По итогам его анализа определены основные риски, присущие площадкам: операционные, правовые и репутационные – в частности, технологические риски площадки, риск непрерывности деятельности, риски, связанные с хранением и обработкой данных, риски мошенничества и другие.

В настоящее время при активном участии Банка России и Минэкономразвития в диалоге с участниками рынка заканчивается подготовка ко второму чтению законопроекта «О привлечении инвестиций с использованием инвестиционных платформ», призванного одновременно создать благоприятные условия для долгосрочного развития краудфандинга, стимулировать развитие сегмента МСП и повысить защиту прав заимодавцев и розничных инвесторов».

3.1.2. Статьи в научных изданиях, посвященные динамике рынка P2P кредитования, а также иных моделей альтернативного кредитования за рубежом и в России:

- **Е.В. ВАСИЛЬЕВА Развитие европейского рынка альтернативного финансирования https://cyberleninka.ru/article/v/razvitie-evropeyskogo-rynka-alternativnogo-finansirovaniya;**
- **О.Ю ПАТЛАСОВ, А.А.ГРАХОВ Краудфандинг и сеть p2p: прогноз взаимодействия и альтернативного финансирования в условиях кризиса https://cyberleninka.ru/article/n/kraudfanding-i-set-p2p-prognoz-vzaimodeystviya-i-alternativnogo-finansirovaniya-v-usloviyah-krizisa.**

3.1.3. Публикации экспертов в СМИ:

- **Bankir.ru – P2P-кредитование вместо банков: выход для малого бизнеса https://bankir.ru/publikacii/20151125/p2p-kreditovanie-vmesto-bankov-vykhod-dlya-malogo-biznesa-10006935/**

«Рынок p2p-кредитования в России достигнет к 2018 году 4,3 млрд рублей, а в целом же его потенциал – не менее 40 млрд рублей, подсчитали в компании «Город денег». Особенно интересны перспективы услуги p2p в кредитовании малого бизнеса, чему будет способствовать дальнейшая консолидация банков и экономический кризис, из-за которых предпринимателям все сложнее получить классический кредит.

Peer-to-peer кредитование – кредитование «от человека человеку», без участия банков, изначально появилось в России в сфере розничного кредитования. Однако экономический кризис создал условия для роста p2p-кредитования малого бизнеса. Сегодня мелкие банки становятся неконкурентоспособными и уходят с рынка. Такова тенденция не только в России: например, в Италии с 2008 года закрылось 118 банков, а в целом в Европе – около 750, такие цифры привел президент General Investment Group и председатель совета директоров ФГ «Город денег» Винченцо Трани. «Европейский, и особенно итальянский, банковский бизнес очень старый, и я вам могу сказать, что никогда ситуация в секторе не была такой тяжелой», – говорит финансист.

Банки постепенно уходят с рынка кредитования малого бизнеса, освобождая эту нишу для небанковских структур.

В свою очередь, крупные банки не могут предоставить малому бизнесу гибкие условия и скорость обслуживания, в которых тот нуждается. Себестоимость банковских услуг растет, что делает нерентабельной выдачу кредитов на небольшие суммы. Банки постепенно уходят с рынка кредитования малого бизнеса, освобождая эту нишу для небанковских структур – МФО, кредитных кооперативов и площадок p2p. Чем интересно p2p-кредитование для заемщиков, инвесторов и организаторов услуги?

Малый бизнес: проще, но дороже

Средний размера кредита в Сбербанке составляет 10 млн рублей, что гораздо выше обычной потребности малого бизнеса. Сравните: средний размер в компании «Город денег» – до 500 тысяч рублей, а в регионах эта сумма может быть еще меньше – до 100 тысяч рублей. Однако банкам работать с такими суммами зачастую не интересно.

Срок рассмотрения заявки в «Городе денег» – до недели, в то время как банки обычно принимают решение в течение месяца. Средний срок кредита – 18 месяцев, а ставка колеблется от 30% до 50% годовых и в среднем составляя около 34%. Она существенно выше, чем та, что предлагают банки. Проблема, однако, в том, что взять такой кредит не так-то и просто. Сегодня, когда банки существенно сокращают свои филиальные сети, у предпринимателей зачастую нет физической возможности добраться до отделения и взять кредит. Когда такая возможность есть, на первый план выступают те самые гибкость и скорость. Пока предприниматели ждут решения банка по кредиту, они иногда занимают средства на площадке p2p.

Инвестор: выгодно, но без гарантий

Суть p2p-кредитования, как известно, состоит в том, что инвесторы кредитуют бизнес напрямую. Кредитор сам выбирает компанию или предпринимателя, в чей бизнес хочет инвестировать средства. Задача платформы p2p в данном случае – предоставить гарантии надежности бизнеса. Проверка компаний происходит по стандарту, разработанному ЕБРР для малого бизнеса стран с развивающейся экономикой. Именно этого стандарта придерживаются и банки при рассмотрении заявки. Необходимое условие

предоставления кредита в «Городе денег» – залог и поручительство. Именно залог помогает просроченным ссудам не уходить в категорию безнадежных.

Историческая просрочка кредитов малого бизнеса – 1%, что делает эту категорию заемщиков наиболее надежной.

Кстати, доля просроченных p2p-кредитов (то есть там, где пропущены два и более платежа) составляет 5%. Винченцо Трани, который начинал работу в России в ЕБРР в 2002 году, говорит, что историческая просрочка кредитов малого бизнеса – 1%, что делает эту категорию заемщиков наиболее надежной. Причина в том, что малые предприниматели дорожат свой репутацией, их компания для них не просто очередная работа, а зачастую дело всей жизни и источник существования семьи.

Тем не менее, для диверсификации риска в компании советуют выдавать взаймы лишь часть необходимых денег. Как правило, один заемщик получает деньги от трех-пяти инвесторов. Это позволяет снизить риски для обеих сторон. Но в любом случае никакой системы страхования, как в случае с банковскими вкладами, в p2p-кредитовании не существует. Об этом необходимо помнить.

Платформа p2p-кредитования: светлые перспективы и возросший риск

Компания-организатор p2p-кредитования получает комиссионный доход с обеих сторон. Например, «Город денег» получает 1% от суммы кредитования от инвестора и 2% – от заемщика. Размер прибыли в компании не раскрывают, ссылаясь на непубличность компании, но представление о масштабах бизнеса можно получить, опираясь на сумму одобренных кредитов, – 515 млн рублей за первые полтора года работы компании.

Надзор в p2p-сфере будет адекватен размеру бизнеса и что ЦБ будет избегать избыточного регулирования подобных структур.

Интерес этого сектора небанковских услуг состоит еще и в том, что Центробанк лишь начинает присматриваться к p2p. Первая квартальная отчетность была направлена в ЦБ меньше месяца назад, рассказала гендиректор компании «Города денег» Елизавета Карпиловская. Первый зампред ЦБ Сергей Швецов на проходящей недавно в Москве конференции, посвященной параллельной банковской системе, подчеркнул, что надзор в этой сфере будет адекватен размеру бизнеса и что ЦБ будет избегать избыточного регулирования подобных структур.

Однако кризис, который дал импульс p2p-кредитованию, одновременно породил и новые риски. Резко возросло мошенничество: если в прежние годы доля отказов при рассмотрении заявок на кредиты от малого бизнеса составляла в банках около 30%, то сейчас специалисты «Города денег» отклоняют 80% заявок.

Перспективы: 1% наличной денежной массы

Кредитованию p2p как явлению всего несколько лет, не только в России, но и во всем мире. Возникший в ответ на финансовый кризис, рынок p2p в США, Великобритании и в Китае вырос на последние пять в 26 раз: с $1,4 млрд до $36,7 млрд. Крупнейшая компания, работающая на этом рынке, американская Lending Club, выдала кредитов на $13 млрд. Потенциал российского рынка оценивается в 40 млрд рублей, или 1% наличной денежной массы, находящейся на руках населения (3,8 трлн рублей, по данным Росстата), приводит свои расчеты «Город денег».

- **Rusbase – Как устроен рынок P2P-кредитования в России и за рубежом https://rb.ru/opinion/p2p/**

«Банковские услуги необходимы, а банки – нет. – Билл Гейтс

P2P кредитование (от peer-to-peer – «друг другу») начало развиваться в 2005 году. Одной из первых в мире такого рода бизнесом стала заниматься английская компания Zopa, которая в настоящий момент является крупным игроком этого рынка в Великобритании. В 2015 году крупнейшая платформа – американский сервис Lending Club – уже является публичной компанией с оценкой более $5 млрд. Всего в этом году через различные сервисы P2P кредитования (так называемые P2P платформы) в мире будет выдано, по оценке Target Ventures, более $20 млрд кредитов.

P2P кредитование – финансовый сервис выдачи займов (совершенно разных – потребительских, бизнесу, ипотечных и многих других), в которых кредитором выступает не банк или кредитная организация, а большое количество физических лиц или институциональных инвесторов. При этом сервис P2P кредитования является платформой, которая объединяет с одной стороны кредиторов, а с другой – заемщиков. Платформа не принимает на себя кредитных рисков – все займы выдаются за счет денежных средств кредиторов. Сервис проводит скоринг заемщиков, оказывает услуги по сбору просроченной задолженности и удобной оплаты по выданным кредитам.

Аристотель в своей книге «Политика» говорит: «Посредники пользуются повсюду наибольшим доверием» – точно так же и в современном мире банки пользуются наибольшим доверием среди тех, кто планирует сохранить заработанные денежные средства или взять их в кредит.

По своей сути банковская организация – лишь посредник между теми, кто вкладывает деньги, и теми, кто берет кредит. Давать деньги друг другу в долг мы боимся, а вот банку доверяем – этот парадокс искореняют сервисы P2P кредитования. При этом, как правило, маржа за такого рода банковское «посредничество» достаточно высока – к примеру, в США депозит можно разместить под 1-2% годовых, а вот получить деньги в кредит возможно лишь под 12-17%. P2P платформа же взимает от 2 до 5% от суммы займа с заемщика и до 1% годовых с кредитора за обслуживание займов. Экономия более чем вдвое – очевидна разница между 11-15% в случае банка и 3-6% в случае P2P платформы.

США, Великобритания и Россия

Наибольшее развитие P2P кредитование получило в США и Великобритании – именно в этих странах сконцентрированы основные платформы, которые, согласно данным из открытых источников, выдают наибольшее число кредитов:

1. Lending Club (США) – в 1Q 2015 выдал $1,6 млрд кредитов
2. Prosper (США) – в 1Q 2015 выдал $600 млн кредитов
3. SoFi (США) – планируют выдать более $2 млрд кредитов в 2015 году
4. Funding Circle (Великобритания) – планируют выдать более $1 млрд кредитов за 2015 год
5. Zopa (Великобритания) – планируют выдать около $1 млрд кредитов в 2015 году
6. RateSetter (Великобритания) – сравним с Zopa по объемам выданных кредитов, по некоторым данным превосходит Zopa.

Успехи России в данном направлении пока скромные. По сути, у нас эта индустрия представлена двумя компаниями – Вдолг.ру и Fingooroo. Насколько известно, у обоих сервисов небольшие показатели выдачи кредитов по сравнению с вышеперечисленными платформами (похожая ситуация наблюдается и во многих других странах). В первую очередь это связано с особенностями работы индустрии кредитования в целом и, самое главное, наличием кредитных бюро с достоверной кредитной историей по заемщикам.

Если централизованное кредитное бюро отсутствует, то человек, не вернувший займ, может сразу получить еще один. В этом случае возникают проблемы – сначала с просроченными задолженностями (мотивация к возврату денег недостаточно высока), а потом и с завышенными процентными ставками: добросовестные заемщики вынуждены платить не только за себя, но и за недобросовестных.

P2P – это не только потребительские кредиты

В связи с тем, что самые большие (а также самые старые и самые известные) P2P платформы, Lending Club, Prosper и Zopa, работают на рынке потребительского кредитования, у большинства людей P2P кредитование ассоциируется именно с потребительскими займами. Однако за последние 3-5 лет в мире появились новые ниши P2P кредитования, которые по своим объемам иногда даже превосходят рынки, на которых работают, например, Prosper и Zopa. Вот некоторые такие ниши:

1. Займы бизнесу – как правило, от $50 тыс до $500 тыс сроком на несколько лет. Есть и более инновационные продукты, которые работают по принципу «кредитной карты для бизнеса», когда компании одобряется определенный лимит. Далее она может брать деньги, отдавать их в любой срок, а проценты платить только за время фактического пользования деньгами. Основные игроки этого рынка – Funding Circle, Biz2Credit, Kabbage.
2. Рефинансирование образовательных кредитов – это отдельная огромная отрасль в США с понятной предпосылкой для возникновения такого бизнеса. Независимо от того, в каком университете ты учишься, государство выдает тебе образовательный кредит по одной и той же ставке, в то время как очевидно, что студент Гарварда имеет принципиально более низкий риск дефолта по сравнению со студентом никому не известного вуза. Эта особенность открывает окно возможностей для рефинансирования образовательных кредитов студентам топовых вузов под более низкую процентную ставку. Основные игроки – SoFi,CommonBond. Логику влияния образования на процентную ставку также имеет UpStart.
3. Рефинансирование дебиторской задолженности – огромная и очень нужная рынку отрасль, которая позволяет небольшим компаниям лучше управлять своим оборотным капиталом. Кредит предоставляется под залог требований по выплате клиентов бизнеса или товаров в обороте. Основные игроки: MarketInvoice,BlueVine, FundBox.
4. Кредиты под залог коммерческой недвижимости или операции fix & flip (покупка, ремонт, перепродажа) – это огромная ниша, которая только начинает свой путь online. Этот рынок в несколько раз крупнее consumer loans, но и сложнее, так как чеки в нем существенно больше. В этом секторе пока отсутствует четкий лидер, но целый ряд компаний претендует на это звание: Realty Mogul, Realty Shares, Patch of Land, Asset Avenue, Lending Home и другие.

5. Ипотечные кредиты под залог жилой недвижимости – это также огромный рынок, однако после кризиса 2008 года он находится под серьезным регулированием. Несколько сервисов только начинают свою работу в таком сегменте, и это выглядит как многообещающая ниша.
6. Другие модели. Например, кредитование с поручительством, когда можно поручиться за того, кому будет предоставлен займ или дать ему рекомендацию – это повлияет на процентную ставку. В этой области, к примеру, лидером является компания Vouch.

Игроки рынка

Рынок кредитования настолько большой, что постоянно появляются новые и новые платформы – даже в давно существующих областях. Например, Marlette Funding (работает в том числе под брендом Best Egg) уже прочно занял место игрока №3 в США в области потребительского кредитования. Основатель PayPal Макс Левчин (Max Levchin) создал компанию Affirm, специализирующуюся на POS кредитовании, которая привлекла уже более $300 млн инвестиций. Существующие гранды тоже выходят на рынок кредитования через интернет – так, Goldman Sachs недавно объявил о выходе на рынок потребительского онлайн-кредитования.

Далеко не все новые компании работают в форме традиционных P2P платформ, так как с ростом популярности кредитования через интернет основными кредиторами на платформах стали институциональные игроки. Партнерство с несколькими крупными компаниями позволяет платформе выдавать до $1 млрд (а в некоторых случаях и более) с последующей секьюритизацией портфеля займов, то есть, превращения их в ценные бумаги.

Несмотря на то, что физические лица не всегда могут инвестировать через P2P платформы, эти сервисы по-прежнему можно причислить к разряду P2P, так как кредитование происходит без банковской организации в роли посредника.

На первый взгляд это может показаться странным, но в последнее время банки также становятся кредиторами на P2P платформах, фондируя существенный объем выдаваемых кредитов. Следует понимать, что для небольшого банка (например, банк с $10 млрд активов – это по-прежнему «небольшой» банк в США) привлечение заемщиков является настоящей проблемой. Им экономически выгоднее заплатить платформе 1% в год за обслуживание «портфеля кредитов», чем привлечь этих заемщиков самостоятельно, а также нести все расходы, связанные с их обслуживанием.

Следуя этой тенденции, в настоящий момент видится, что будущее P2P платформ лежит в более тесной интеграции с дешевыми и стабильными источниками капитала (банки) для наращивания выдачи кредитов и постепенного снижения процентных ставок. При этом ведущие платформы, как правило, будут стараться поддерживать долю инвесторов физических лиц на значимом уровне. Это устойчивая база кредиторов, которая менее подвержена панике в случае ухудшения экономической ситуации.

В России, на мой взгляд, будущее лежит в области кредитования под залог активов.

Пока у нас нет по-настоящему развитого кредитного бюро, агрегирующего информацию о заемщиках, а отчетность компаний не отражает реальную суть происходящего у них внутри, эффективное потребительское кредитование и кредитование

бизнеса через интернет невозможно. При этом кредитование под залог активов является существенно более безопасным и понятным для большинства российских кредиторов».

- **Ведомости – Как одолжить денег незнакомому другу https://www.vedomosti.ru/finance/blogs/2017/02/06/676340-odolzhit-neznakomomu-drugu**

«В России развитие рынка кредитования друг друга тормозится регулированием и недостатком информации

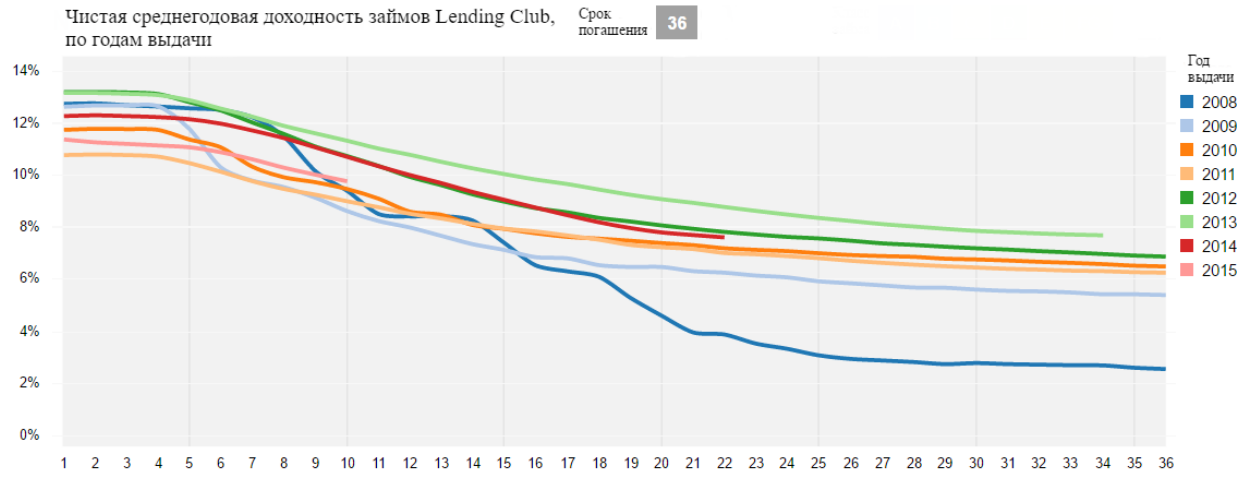
P2P-кредитование (peer-to-peer, т. е. «от равного к равному») – новый способ взаимодействия инвесторов и заемщиков, который позволяет предоставлять кредит без вовлечения финансового института в качестве посредника, что приводит к упрощению всего процесса и существенной экономии времени для участников. За счет переноса всех действий на высокотехнологичные онлайн-платформы p2p-компании экономят на расходах на персонал, аренде офисов и прочих расходах, что позволяет предложить заемщикам и инвесторам более выгодные ставки. Кроме того, p2p-платформы не принимают депозитов; это позволяет избегать затрат на создание резервов, что выгодно отличает их от конкурентов из банковской сферы.

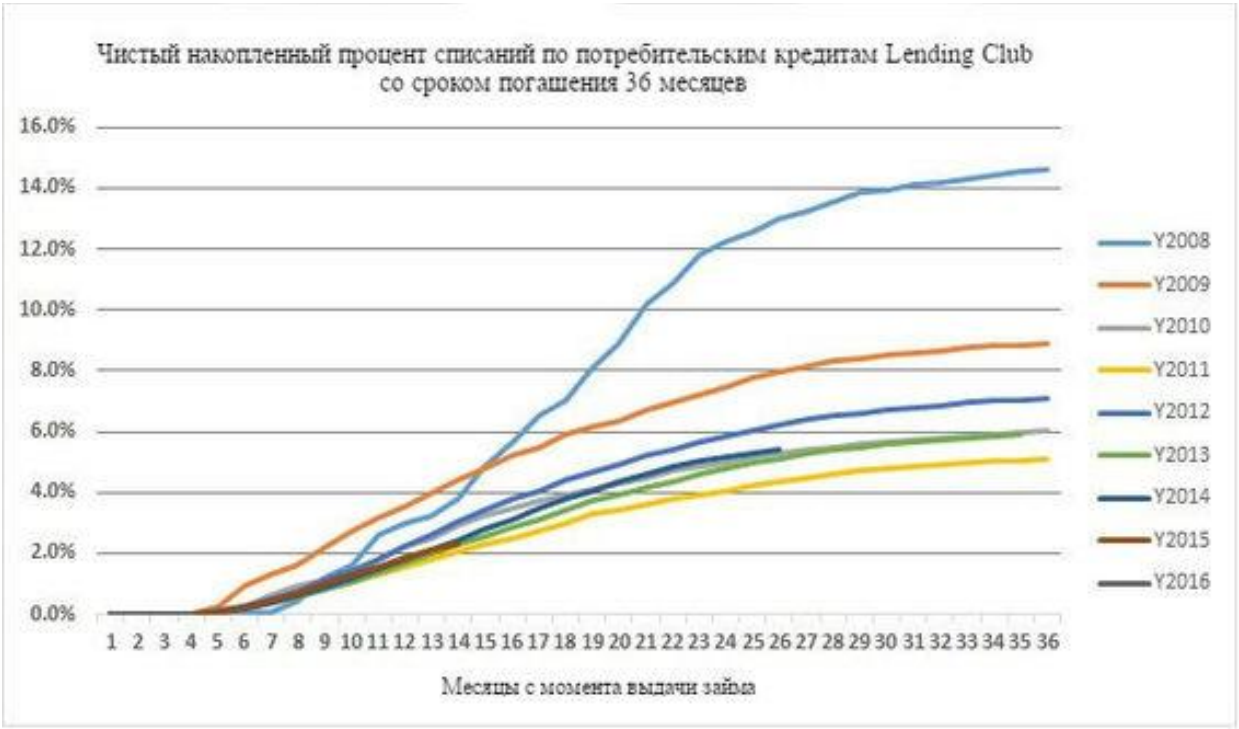
Возможности p2p-кредитования стали особенно очевидны, когда после кризиса 2008–2009 гг. банки ужесточили требования к заемщикам, а сроки рассмотрения заявок на кредиты увеличились.

Первой p2p-платформой стала английская Zopa, которая появилась на рынке в 2005 г. и с тех пор выдала займов более чем на 1,9 млрд фунтов ($2,4 млрд). В 2006 г. p2p-кредитование начало развиваться в США: тогда была основана платформа Prosper (сейчас является второй по величине в США с общей суммой выданных кредитов более $8 млрд), а уже в следующем году появилась компания Lending Club, которая через семь лет провела IPO и была оценена в $5,4 млрд. Постепенно p2p-кредитование распространилось и в других странах, сейчас настоящий бум переживает китайский рынок – объемы выдачи кредитов таких игроков, как Lufax, в несколько раз превосходят даже Lending Club. Мировой объем рынка p2p-кредитования превысил $50 млрд в 2015 г. и, по разным прогнозам, достигнет $300–400 млрд уже в 2020 г.

Развитие рынка не было гладким: против Lending Club и OnDeck, двух первых публичных компаний сектора, были поданы многочисленные судебные иски, касающиеся в основном сокрытия ими важных для инвесторов данных при проведении IPO. Вспоминается также история с Ezubao – одной из крупнейших p2p-платформ в Китае, которая оказалась финансовой пирамидой. Эти события значительно повлияли на индустрию в целом и негативно отразились на цене акций публичных p2p-компаний; так, капитализация Lending Club сперва превысила $8 млрд, а потом снизилась до $2 млрд, где и находится сейчас.

Тем не менее, так как качество займов на платформах высоко и уровень дефолтов остается на стабильно низком уровне, компании продолжают расти, а рынок – развиваться. Графики ниже демонстрируют чистую доходность и процент списаний (данные на конец III квартала 2016 г.) по займам Lending Club в зависимости от года выдачи. Как видно, с 2010 г. дефолты не превышали 8%, а доходность стабильно держалась выше 6%.





Вместе с ростом числа платформ p2p-кредитования появляются игроки, деятельность которых направлена на обслуживание уже существующих p2p-платформ. Яркий пример – компании Orchard, PeerIQ, российская Blackmoon Financial Group, которые предоставляет институциональным инвесторам доступ к онлайн-платформам. p2p-кредитование привлекает инвесторов своей доходностью: инвестируя в займы, можно зарабатывать от 7 до 12% в валюте с учетом дефолтов и контролируемыми рисками – это существенно больше доходности аналогичных по рискованности инструментов.

Российский сектор развивается куда медленнее. Первые p2p-компании, «Кредитвсем» и «Биржа кредитов», вышли на рынок в 2010 г. «Биржа кредитов» перешла на модель онлайн-кредитования покупателей интернет-магазинов; по запросу «Кредитвсем», в свою очередь, сегодня можно найти огромное количество одноименных

сервисов, которые не имеют отношения к оригинальной компании. Компания «Вдолг.ру», созданная в 2012 г. при участии banki.ru и фонда Runa Capital, столкнулась с проблемами регулирования и в апреле 2016 г. приостановила выдачу займов; сейчас регистрация новых пользователей на платформе все еще не производится.

Проблемы российского рынка p2p-кредитования прежде всего связаны с отсутствием развитой скоринговой системы всего населения в одинаковом и сравнимом формате (например, такой, как FICO в США, агрегирующей и анализирующей данные трех основных кредитных бюро). Пока официальная отчетность компаний и данные о заемщиках не всегда соответствуют реальности, эффективное p2p-кредитование не представляется возможным. При таких условиях в России с большей вероятностью получит распространение схема кредитования с обратным выкупом, при которой «заемщик» продает актив по сниженной стоимости, обязуясь выкупить его с процентами. Мешает и несовершенство законодательства: выдача займов на платформах может быть расценена как банковская деятельность.

Доступ российских инвесторов к вложениям в p2p-кредиты ограничен – иностранные платформы, руководствуясь местным законодательством, не принимают инвестиции от иностранцев. Однако получить доходность при инвестициях в P2P-кредиты возможно, вкладываясь в специализированные фонды, – у них отсутствуют какие-либо ограничения на национальность инвесторов. Схема выглядит следующим образом: инвестор приобретает паи фонда, а фонд уже в свою очередь инвестирует в займы на p2p-платформах. В России сейчас своих представителей имеет только американский фонд Prime Meridian, который является одним из крупнейших в этой индустрии с активами под управлением более $350 млн.

Безусловно, у инвестиций в p2p-кредиты есть и свои риски, которые необходимо принимать в расчет. Так, эта индустрия еще ни разу не проходила через масштабный кредитный кризис. Ряд исследований говорит о том что даже при таком кризисе, как в 2008 г., доходность хорошо подобранного и диверсифицированного портфеля p2p-займов не должна уходить значительно ниже нуля, однако на практике такой проверки этот класс активов еще не проходил».

- **Forbes – В одной лодке: как платформы p2p-кредитов сотрудничают с банками**
  http://www.forbes.ru/tehnologii/340171-v-odnoy-lodke-kak-platformy-p2p-kreditov-sotrudnichayut-s-bankami

«Представители традиционной банковской инфраструктуры могут работать с площадками взаимных займов – как агенты или как сокредиторы. В Европе такое сотрудничество уже набирает обороты.

Информационные технологии открывают возможности для формирования новых небанковских финансовых институтов, новых финансовых услуг и новых методов оказания этих сервисов. То, что вчера считалось немыслимым, сегодня становятся обыденным. Банкам приходится тяжело: с одной стороны, они распоряжаются денежными средствами своих клиентов и обязаны тщательно взвешивать риски и условия предоставления финансовых средств взаймы. С другой стороны, когда речь заходит о микро-финансировании, традиционные банковские продукты оказываются слишком громоздкими

и неудобными – тогда клиенты банков начинают искать альтернативы. В этом смысле появление P2P-платформ совместного кредитования было лишь вопросом времени, и такие платформы действительно становятся все масштабнее.

Возможность кредиторов и заемщиков договариваться друг с другом напрямую, устанавливая приемлемые соотношения рисков и доходности, стала обеспечиваться средствами автоматизации платформы. Такие сервисы сейчас крайне востребованы: нет необходимости собирать большой комплект документов и идти в банк, потому что сервисы работают через дистанционные каналы; не надо открывать дополнительный счет – можно использовать открытые счета в обслуживающих банках; сервисы очень быстро реагируют на запросы и потребности своих клиентов. И, наконец, P2P-платформы позволяют получать займы без обеспечения, что крайне актуально для сегмента малого и микро- бизнеса.

Интеграция банков с P2P-платформами VS собственные разработки

P2P-платформы снижают издержки и захватывают большую долю рынка. Многочисленные попытки банков выстроить эффективный процесс кредитования малого бизнеса заканчивались неудачей. Этот сегмент рынка до сих пор привлекает банки, но требует слишком больших затрат, связанных с технологическими особенностями процесса обработки заявок. Малый бизнес, в отличие от крупного, слишком разнообразен, слишком неочевиден и требует слишком больших усилий для изучения, чтобы «пакетные продукты» давали результат. В итоге кредитование малого бизнеса не показывало ожидаемой нормы прибыли, либо критерии оценки рисков были затянутыми настолько, что продукт просто не находил своего клиента.

Платформы P2P-кредитования находятся в более выгодном положении по сравнению с банками из-за отсутствия жестких регуляторных требований. Они могут предложить конечным пользователям решения в тех клиентских секторах, которыми часто пренебрегают банки. Основной задачей, которую решают создатели P2P-платформ, является минимизация издержек, связанных с привлечением клиентов. Но P2P-платформы появились в России недавно и не получили пока достаточной известности среди российского потребителя. Поэтому любая P2P-платформа будет вынуждена прикладывать гораздо больше усилий на привлечение клиента, чем затрачивает классический банк.

Среди возможных способов взаимодействия классических банков и P2P-платформ я бы выделил следующие направления:

1. Агентская модель взаимодействия. Банк выступает агентом, который приводит клиентов. Им отказано в финансировании по нормативам и условиям программы кредитования банка, но они могут получать финансирование по условиям продукта P2P-платформы. Банк получает дополнительное комиссионное вознаграждение при минимуме затрат на обслуживание клиентов и без рисков финансирования. P2P-оператор получает клиентов без существенных затрат на привлечение, ограничиваясь выплатой банку комиссионного вознаграждения. Все транзакционные доходы по обслуживанию клиента также остаются на стороне Банка.
2. Кобрендинговая программа. Банк выступает не только поставщиком клиентов – потенциальных заемщиков, но и распространяет информацию о возможности размещения свободных средств среди клиентов-кредиторов. Для этого банку

потребуется провести аккредитацию рисковой модели P2P-оператора в силу возникновения определенных репутационных рисков для банка.

3. Со-финансирование. Банк выделяет определенный объем свободных средств и выступает в качестве кредитора в проектах, финансируемых P2P-платформой.

Поскольку рынок P2P-кредитования в России является достаточно молодым, здесь еще рано говорить, что гарантированно «выстрелит». Но с высокой степенью достоверности можно отразить те черты P2P-платформ, которые будут наиболее понятны и востребованы банками.

- Наличие модели оценки рисков, понятной и приемлемой для банков. Чем более надежная и проверенная на практике модель используется для оценки заемщиков P2P-платформы, тем выше вероятность успешного взаимодействия с банками после прохождения процедуры аккредитации модели/платформы.
- Наличие ИТ-платформы с необходимым уровнем автоматизации. Чем более совершенная и функционально полная платформа будет использована P2P-оператором, тем легче она может быть интегрирована в банковскую ИТ-среду, в особенности с учетом требований масштабируемости бизнеса. Вопрос возможности наращивания производительности ИТ-системы при увеличении объемов операций рассматривается банками как один из ключевых.
- Опыт и профессионализм команды P2P-платформы.

На более развитых зарубежных финансовых рынках банки и P2P-платформы взаимодействуют совсем по-другому. Банки поняли потенциал представителей новой одноранговой экономики и не хотят упускать этот сегмент дополнительной прибыли. Так, в конце прошлого года одна из наиболее известных платформ в этой сфере, американская OnDeck, объявила о стратегическом сотрудничестве с JP Morgan для осуществления программы кредитования малого бизнеса. Для OnDeck проект даст возможность расширить кредитный портфель (который и без того составлял более $5 млрд., а количество выданных займов – более 60 000), банку – получить доступ к технологии, которая значительно повысит скорость принятия решения о выдаче займа.

Британский Metro Bank теперь выдает займы через платформу взаимного кредитования Zopa. Подписанный в 2016 договор, согласно которому банк получил возможность выдавать займы через веб-сервис персонального кредитования, стал первой сделкой такого рода в Соединенном Королевстве. Кроме того, в Великобритании подобные формы сотрудничества поощряются даже регулятором – он подталкивает банки к тому, чтобы передавать другим игрокам финансового рынка компании, которым те отказали в кредите. Банк Santander договорился с компанией Funding Circle о передаче клиентов из малого и среднего бизнеса, которые банку не интересны, а взамен Funding Circle будет предлагать клиентам открывать в этом банке текущие счета и другие услуги, которые не может оказать самостоятельно как компания без банковской лицензии.

Такие крупные финансовые организации, как Morgan Stanley, Citygroup и Wells Fargo через свои дочерние венчурные структуры инвестируют в Lending Club, при этом JPMorgan Chase инвестирует в Prosper. Goldman Sachs также создал публичную небанковскую компанию – Goldman Sachs BDC, которая занялась инвестированием в портфели P2P-

кредитования среднего бизнеса, и объявил о разработке цифровой платформы, которая позволила бы выдавать ссуды в размере $15 000 – $20 000.

На текущий момент в открытых источниках отсутствуют количественные оценки эффективности партнерства зарубежных банков и P2P-платформ, но уже сейчас ясно одно – рынок будет меняться. Несмотря на то, что многие компании, работающие в сегменте P2P, активно набирают обороты, со стороны многих игроков рынка все чаще звучат предложения, что в дальнейшем они будут консолидироваться с банками. Да и банки разглядели в провайдерах P2P-кредитования возможных партнеров. За десять лет существования сегмент получил такое развитие, что у банков не осталось сомнений в их жизнеспособности и перспективности.

К сожалению, в настоящее время на российском рынке нет примеров полноценной интеграции P2P-платформ и банковских систем, за исключением проприетарной системы «Альфа-Поток», разработанная Альфа-Банком. Поэтому делать однозначные выводы о результатах такой интеграции пока рано, но многие крупные банки проявляют интерес к взаимодействию такого рода. Вполне возможно, что через некоторое время эта технология войдет в число обычных банковских инструментов».

3.2. Риски P2P кредитования

3.2.1. Оценка рисков площадок P2P кредитования экспертами органов банковского надзора

- **Информация об оценке рисков площадок P2P кредитования Банком России**
  https://finance.rambler.ru/economics/34473951-tsb-schitaet-riskami-p2p-ploschadok-neprozrachnost-moshennichestvo-i-otsutstvie-garantiy/

«ЦБ считает рисками p2p-площадок непрозрачность, мошенничество и отсутствие гарантий

Банк России перечислил основные риски p2p-площадок. В их числе непрозрачность бизнес-модели, мошенничество и отсутствие гарантий возврата займа, сообщили RNS в пресс-службе регулятора.

«Отсутствует уверенность, что «виртуальный контрагент» по p2p-площадке реально существует или что для займа не использованы данные третьего лица без его ведома», – комментирует представитель ЦБ риск неверной идентификации.

Вторым риском является качество скоринга клиента – p2p-площадка не несет ответственность за качество скоринга и достаточность мер, предпринимаемых против мошенничества, а также за способность заемщика вернуть долг.

Также сомнения регулятора вызывает качество проверки бизнес-проекта – p2p-площадки сами определяют требования к оценке документа, проверке бизнес-модели и документов. «При наличии якорного инвестора острота проблемы снижается», – отмечает регулятор.

Четвертым риском является непрозрачность модели: «Клиент видит в интернете „витрину“, но не имеет реальной возможности проверить корректность данных юридического лица, создавшего p2p-площадку».

Регулятор отмечает, что p2p-площадки не предоставляют никаких гарантий возврата займа. В случае просрочки или невозврата, отсутствуют эффективные механизмы взыскания долга. Перспективу обращения в суд ЦБ считает «сомнительной» в силу отсутствия «живых» документов.

«В случае использования площадки как «ширмы» для создания финансовой пирамиды весьма затруднительно выявить наличие признаков мошенничества и отказаться от инвестирования», – описывают в ЦБ риск мошенничества.

В случае технических проблем или внезапного прекращения работы краудфандинговых площадок по инициативе организатора у заимодавцев и заемщиков возможны проблемы с регистрацией права или возвратом инвестиций.

«Особо внимательно следует оценивать риски вложений, если площадка зарегистрирована не в России, а за рубежом, но рекламирует свои услуги на русском языке для граждан России. В этом случае, при возникновении проблем с площадкой, возврат вложенных средств будет крайне затруднен», – подводят итог в ЦБ.

p2p-кредитование (peer-to-peer кредитование) – кредитование физическими лицами друг друга без участия финансовых посредников в виде банков. Осуществляется на основе специализированных интернет-сайтов.

Банк России может выступить с предложением по регулированию рынка краудфандинговых и краудинвестинговых площадок до конца 2016 года, сообщили RNS в пресс-службе регулятора».

- **А. Ткачев, В. Баталко. Возможности и риски краудфандинга и P2P-займов. Банкаўскі веснік, МАЙ 2018:**
  Полный текст статьи содержится по адресу:
  https://www.nbrb.by/bv/articles/10516.pdf

В статье специалисты Управления финансовой стабильности Национального банка Республики Беларусь рассматривают механизмы деятельности отдельных P2P-платформ, возможности и риски P2P-финансирования. В качестве основных рисков называются:

1. Асимметрия информации.

2. Отсутствие гарантии возврата инвестиций

3. Передача кредитного риска инвесторам.

4. Риск мошенничества со стороны интернет-площадок при ранжировании займов по уровню риска и процентных ставок.

5. Недиверсифицированный кредитный риск у инвестора (в сравнении с депозитом в банке).

6. Процентные ставки могут не компенсировать вероятность дефолта должника.

7. Риск мошенничества и кражи идеи проекта.

8. Отсутствие специальных нормативных требований, выходящих за рамки стандартных правовых требований для ведения бизнеса.

- **Report on lending-based crowdfunding: risks, drivers and potential regulatory approaches:**

https://eba.europa.eu/documents/10180/983359/EBA-Op-2015-03+%28EBA+Opinion+on+lending+based+Crowdfunding%29.pdf

Доклад является приложением к документу Европейского банковского управления Opinion of the European Banking Authority on lending-based crowdfunding (EBA/Op/2015/03, 26 February 2015).

Доклад представляет анализ основных рисков P2P кредитования; идентифицирует группы рисков отдельно для кредиторов, заемщиков, операторов платформы; предлагает регулятивные подходы к снижению рисков.

3.2.2. Материалы СМИ, обращающие внимание на отдельные аспекты рисков P2P кредитования

- **Коммерсант – Граждане не доверяют друг другу деньги**
  https://www.kommersant.ru/doc/3842950

«Объемы P2P-кредитования упали на треть

Рынок краудфандинга по итогам девяти месяцев текущего года показал рост, однако только за счет финансирования компаний и ИП, объем финансирования граждан гражданами упал на треть. Люди не доверяют потенциальным заемщикам–физлицам в связи с высоким уровнем невозвратов по ранее выданным P2P-ссудам. Эксперты отмечают, что если в ближайшем будущем у площадок не появится больше данных для оценки кредитоспособности граждан, данный сегмент рынка может вовсе исчезнуть.

По данным Банка России, за три квартала текущего года объем рынка краудфандинга превысил 11,14 млрд руб., что почти в 1,5 раза больше, чем за аналогичный период 2017 года.

Банк России определяет краудфандинг как привлечение инвестиций гражданами или коммерческими организациями с использованием интернет-платформ. К его разновидностям относят краудлендинг (P2P – кредитование граждан гражданами, P2B – юрлиц гражданами, B2B – юрлиц юрлицами), краудинвестинг (финансирование с помощью продажи долей и акций или по договору займа) и сектор rewards (финансирование в обмен на нефинансовое вознаграждение).

Более 95% всего рынка краудфандинга приходится на краудлендинг. За девять месяцев 2018 года суммарный объем сделок в этом сегменте вырос до 11,01 млрд руб. Но рост обеспечило исключительно финансирование юрлиц. А вот граждане, похоже, перестали доверять друг другу. Объем сделок в сегменте P2P-кредитования снизился на треть – с 149,7 млн руб. до 104 млн руб. По мнению регулятора, это, вероятно, отражает невысокую привлекательность данного сегмента для инвесторов, в том числе из-за существенных рисков дефолта заемщиков-физлиц.

Действительно, статистика невозвратов на рынке взаимного кредитования граждан выглядит неутешительно. По словам главы краудлендинговой площадки Penenza Дмитрия Пангина, рынок P2P остается крайне рискованным. «Если риск просрочки в сегментах P2B и B2B находится в пределах 8–10% в среднем по рынку, то по P2P-кредитованию он близок к 50%», – уточняет он. «Заемщики в первую очередь идут за потребкредитом в банк, если там не дают, то в МФО, и уже в последнюю очередь – на платформу P2P, – отмечают в

Ассоциации операторов инвестиционных платформ. – Риск для инвестора в P2P в том, что у него нет запаса ликвидности, например, как у микрофинансовых организаций, для того чтобы компенсировать высокий уровень просрочки». Физлица наконец осознали настоящие масштабы риска дефолта своих заемщиков, говорит аналитик ИК «Алор Брокер» Алексей Антонов. «Они поняли, что не умеют с этими дефолтами работать, не умеют взыскивать средства в судебном порядке и не хотят этим заниматься, потому что затраты на взыскание перекрывают те скромные проценты, которые они зарабатывают по небольшому числу успешных займов», – продолжает эксперт.

При этом данных для оценки потенциальных заемщиков P2P-площадок крайне мало. По словам Дмитрия Пангина, если законодательно не будут внедрены инструменты, дающие P2P-площадкам доступ к источникам данных о расходах-доходах физлиц (не только кредитные истории, но и данные о долгах граждан по ЖКХ, налоговой задолженности, алиментах, реальных доходах), этот сектор рынка краудфинансов в России перестанет существовать в перспективе ближайших лет.

Впрочем, несмотря на резкое сжатие рынка взаимного кредитования граждан, перспективы у краудфандинга в целом неплохие. По прогнозам экспертов, по итогам 2019 года рынок краудфинансов достигнет 20–23 млрд руб., где основную часть займет B2B-кредитование. В ЦБ также ожидают роста рынка: «В 2019 году ожидается приход крупных игроков сегментов P2B и B2B, что может оказать существенное влияние на рынок в целом». Сейчас выход крупных площадок на рынок сдерживает правовая неопределенность в части привлечения займов через краудфандинговые площадки, отмечают там. Законопроект о регулировании краудфандинговых платформ был одобрен Госдумой в первом чтении в середине мая (см. “Ъ” от 22 мая). По словам главы комитета Госдумы по финансовому рынку Анатолия Аксакова, во втором чтении проект закона планируется рассмотреть и принять в начале 2019 года».

- **РБК – Новые ростовщики: стоит ли вкладывать деньги в сервисы взаимных кредитов**
  https://www.rbc.ru/money/07/06/2016/575704d19a79473ea7a4a786

«Сервисы p2p-кредитования дают возможность ссужать деньги под несколько десятков процентов годовых. Каковы риски?

Взаимное кредитование (peer-to-peer, или p2p-кредитование) в России почти не развито, несмотря на то что 59% россиян имеют хотя бы один кредит. По данным ЦБ, в 2015 году совокупный объем портфелей краудфандинговых площадок (а именно к нему ЦБ относит сервисы по взаимному кредитованию) составил около 170 млн руб. Для сравнения: микрофинансовые организации в 2015 году выдали почти 140 млрд руб. займов, а банки – 10,7 трлн руб. кредитов частным клиентам.

Первая российская p2p-площадка открылась в 2011 году. Компанию «Вдолг.ру» основал Антон Тарасов вместе со своими коллегами-банкирами и коллекторами. Тарасов, несколькими годами ранее создавший брокерский бизнес, который аккумулировал заявки на кредиты для банков, в какой-то момент решил исключить кредитные организации из этой цепочки. К 2013 году, по его словам, стали появляться похожие сервисы.

ЦБ, который с прошлого года анализирует эти сервисы, сообщил РБК, что площадки

добровольно отчитываются о результатах своей работы, но данные не раскрыл. Отчетность сдают семь компаний, рассказала Ольга Святченко, генеральный директор сервиса Fingooroo. Кроме ее компании перед ЦБ отчитываются «Вдолг.ру», «Город денег», Loanberry, Fundico, «БезБанка» и Webmoney.

Как это работает

Все эти сервисы предоставляют площадку для заемщиков и их кредиторов и сводят их напрямую. И в этом ключевое их отличие от МФО или банков, которые выдают кредиты самостоятельно. Это позволяет инвесторам в p2p-кредиты делать минимальные инвестиции, в то время как в МФО, регулируемые законодательством, можно вложить минимум 1,5 млн руб. «Эти сервисы позволяют взять в долг или дать взаймы через интернет незнакомым людям», – объясняет Святченко из Fingooroo.

Площадки, впрочем, оказывают различные дополнительные услуги инвесторам – например, оценивают кредитную историю заемщиков. Шесть опрошенных РБК p2p-компаний заявили, что в обязательном порядке запрашивают информацию в бюро кредитных историй, а до этого проверяют документы, которые предоставляет заемщик при регистрации. «Мы проверяем данные паспорта, СНИЛС, ИНН и узнаем, нет ли задолженности перед службой судебных приставов», – рассказывает специалист «БезБанка» Галина Крылова.

Если документы недействительны или задолженность перед ФССП больше 10 тыс. руб., заемщикам отказывают в регистрации, продолжает она. Около 80% потенциальных заемщиков, по данным «Вдолг.ру» и «Город денег», при таком подходе не проходят проверку. По ее итогам заемщики получают кредитный рейтинг. Он может иметь несколько градаций, например девять в компании «Вдолг.ру» (от A до H) или 13 в компании Loanberry (от A1 до E).

«Вдолг.ру» также при проверке определяет ставку, по которой заемщик может взять деньги. Остальные компании предоставляют только ориентировочную ставку – окончательную определяет уже тот, кто ссужает деньги.

У некоторых сервисов есть и собственные службы взыскания долгов. «Кредитор не знает личные данные заемщика, он может видеть только общую информацию, например город, в котором живет заемщик. Контакты заемщика мы раскрываем только в том случае, если он перестает платить. И лишь после того, как с заемщиком поработают наши службы взыскания и коллекторы», – говорит Тарасов из «Вдолг.ру».

Какие условия предлагают сервисы по взаимному кредитованию:

	Fingooroo	«Город денег»	«Вдолг.ру»	Fundico
Минимальная и максимальная сумма вложений, тыс. руб.	3–150	50–10 000	от 0,5	1–300
Средняя сумма займа в мае, тыс. руб.	20	700	25	450
Минимальная и максимальная ставка по займам, % годовых	36,5–547,5	25–45	22–365	17–41
Средняя ставка по займу, % годовых	35	35	36	29,5
Минимальный и максимальный срок выдачи займов	2 нед. – 6 мес.	3 мес. – 36 мес.	1 нед. – 18 мес.	1 мес. – 12 мес.
Комиссия с кредиторов, %	нет	1	3*	нет
Доля просроченных займов более 90 дней, %	12–15	2	16,5	н.д.

* При выводе средств
** При займах более 10 тыс. руб.

Источник: данные компаний

».

- **Московский центр Карнеги – Как китайский рынок p2p-кредитования стал гигантской пирамидой**
  https://carnegie.ru/commentary/77382

«Рынок p2p-кредитования в Китае рушится с невероятной скоростью. Каждый день в стране закрывается в среднем три-пять p2p-платформ. С конца июня обанкротилось более 260 компаний. Обвал рынка, который аккумулировал $218 млрд почти у пяти миллионов инвесторов, уже вызвал социальные протесты.

Утром 6 августа в районе Сичэн (西城区) в Пекине было необычно много полицейских. Часть улицы, где находится офис Комиссии по регулированию банковской и страховой деятельности КНР (КРБСД), была оцеплена. Почти у всех проходящих мимо людей спрашивали удостоверение личности. И некоторых по результатам проверки задерживали и сажали в полицейские автобусы.

Задерживали пострадавших вкладчиков p2p-платформ (peer-to-peer кредитование, где участники дают друг другу займы без посредничества банка), которые шли на митинг к офису КРБСД. Большинство протестующих были задержаны за несколько дней до планируемой акции, некоторых иногородних обманутых вкладчиков полиция снимала прямо с поезда по пути в Пекин. Тех немногих, кто все-таки смог добраться до района Сичэн, вязали на подходе к офису КРБСД.

Очевидно, что полиция знала о готовящейся акции протеста, более того, знала поименно всех участников, которых, по оценкам организаторов, должно было быть около десяти тысяч человек. Подвели протестующих, скорее всего, новые технологии. Акция в Пекине организовывалась через мессенджер WeChat. По-видимому, полиция отслеживала переписку пользователей в мессенджере. Задержанных вскоре отпустили, напомнив о незаконности проведения несанкционированных акций. Им посоветовали отстаивать свои права «законными методами».

Через несколько дней после несостоявшегося митинга Канцелярия руководящей группы по специальному управлению рисками в сфере интернет-финансов разработалапакет из десяти мер, направленных на урегулирование кризиса p2p-платформ. Эти меры, в частности, предписывают местным властям открыть «окна коммуникации» с пострадавшими вкладчиками, запретить создание новых p2p-платформ и усилить проверку и контроль за уже действующими платформами, определить рамки ответственности компаний и их акционеров в соответствии с законом о банкротстве, разработать процедуру банкротства для компаний.

Также меры призывают бороться законными методами с неплательщиками по своим обязательствам, в том числе включать их в черные списки в рамках системы социального кредита (единой системы оценки благонадежности физических юридических лиц, которая заработает в полную силу по всей стране к 2020 году).

Впрочем, как пишет Мартин Чорземпа из Института мировой экономики Петерсона, нового в этих мерах мало. Они скорее призваны заставить местные правительства выполнять разработанное ранее центральными властями законодательство в сфере p2p. Чорземпа отмечает, что у КРБСД всего три штатных сотрудника, которые отвечают за разработку регулирования тысяч платформ. Поэтому, конечно, центр за всем уследить не может, и значительная часть контролирующих функций ложится на местные власти.

Причины кризиса

Платформы p2p были придуманы не в Китае, но именно здесь этот рынок завоевал наибольшую популярность. С 2007 по 2015 год он рос почти на 234% в год. В 2015 году число p2p-платформ переваливало за 3500. С тех пор их количество стало сокращаться (хоть и не было такого обвала, как этим летом). Но даже сейчас в Китае около 1500 p2p-платформ. Для сравнения: в Великобритании (родине p2p) всего сто подобных платформ, в США – около трехсот.

Власти КНР поначалу никак не препятствовали развитию этого рынка и даже, напротив, поддерживали его. Госсовет в июне 2015 года опубликовал «Руководящие мнения по активному стимулированию концепции Интернет+» (国务院关于积极推进«互联网+»行动的指导意见), где, в частности, дается четкое указание «активно развивать глубину и широту инноваций в сфере финансовых услуг в интернете, а также нормативно развивать интернет-кредитование и операции по предоставлению потребительских кредитов в интернете».

Дело в том, что традиционные банковские продукты в массе своей недоступны заемщикам. Банки с охотой выдают кредиты (пусть часто и на сомнительные с точки зрения экономики проекты) государственным корпорациям, потому что понимают, что в случае чего за них ответит государство. А вот малый и средний бизнес часто остается не у дел. Тем более это касается потребительского кредитования.

Кредитная история в Китае есть лишь у 320 млн человек – около 20% населения. Поэтому для среднестатистического китайца получить кредит в китайском банке – практически невозможная задача.

В традиционной банковской системе плохо обстоят дела и для вкладчиков. Ставки по депозитам китайских банков не превышают 2%. При этом индекс потребительских

цен колеблется от 2% до 3%. Получается, что, вкладывая деньги в банк, население кредитует банки по отрицательной процентной ставке.

Кредитование p2p, с одной стороны, давало новые инвестиционные возможности для людей. С другой стороны, позволяло получить финансирование тем, кто не мог кредитоваться в банках. Это было на руку властям хотя бы потому, что, с одной стороны, рост кредитной массы стимулировал деловую активность и потребление, чего так не хватало для трансформации модели экономического роста, о которой говорят уже много лет. С другой – это снимало нагрузку и какие-либо риски с китайской банковской системы.

В начале 2016 года прошла первая волна дефолтов p2p-платформ. Самый одиозный случай – платформа Ezubao, которая оказалась обычной финансовой пирамидой. Компания увела $7,3 млрд у 900 тысяч инвесторов. С этого момента финансовые власти Китая стали более пристально рассматривать рынок p2p. И выяснилось, что в Китае он совсем не похож на классический рынок p2p в других странах.

По идее p2p-компания – это лишь посредник в схеме «заемщик – кредитор». Ее роль сводится к тому, чтобы за определенную плату свести друг с другом тех, кто хочет дать деньги в долг, с теми, кто их хочет получить. Компания может помочь инвесторам проанализировать кредитные риски и просчитать оптимальную ставку процента. Однако решение об инвестировании принимает сам кредитор. Никаких решений, гарантий доходности и возврата средств и других рисков платформа на себя не берет.

Но в Китае p2p-платформы стали играть роль квазибанковских структур. Они аккумулировали средства инвесторов и гарантировали им фиксированную (причем очень высокую) доходность. Затем компании просто вкладывали средства инвесторов в те отрасли, для которых недоступно банковское кредитование. Так, значительный объем p2p-инвестиций шел на проекты в сфере недвижимости. Мартин Чорземпа даже указывает, что некоторые p2p-платформы были тесно связаны с местными правительствами, которые с их помощью финансировали государственные проекты.

Но для того чтобы гарантировать доходность, выдавать кредиты на длительный срок, привлекая при этом краткосрочные депозиты и не допуская разрыва ликвидности, компания должна формировать обязательные резервы и вообще попадать под довольно жесткое банковское регулирование. Платформы p2p не являются банками, поэтому любые подобные действия крайне рискованны и имеют признаки финансовой пирамиды. Стало понятно, что отрасль нужно как-то регулировать.

Меры регулирования

В августе 2016 года КРБСД опубликовала правила (网络借贷信息中介机构业务活动管理暂行办法), по которым физические лица не могут занимать более 200 тысяч юаней (около $30 тысяч) на одной p2p-платформе, а общая сумма долга по всем платформам не должна превышать 1 млн юаней (для юридических лиц эти пороговые значения выше в пять раз).

Кроме того, p2p-платформам запретили аккумулировать капитал и заниматься предоставлением финансовых услуг – например, управлением активами. Каждая p2p-компания должна вести свою деятельность исключительно через депозитарный банк, причем для каждой p2p-платформы – только один. Это значит, что все средства,

полученные p2p-платформой от кредиторов, должны сначала поступить в банк и только после этого направляться заемщикам.

В апреле этого года Канцелярия руководящей группы по специальному управлению рисками в сфере интернет-финансов выпустила новый документ: «Уведомления об усилении интенсивности нормализации операций по управлению активами через интернет и налаживанию работы по контролю» («**关于加大通**过互联网开展资产管理业务整治力度及开展验收工作的通知»). В них, в частности, говорится, что действующие p2p-платформы должны до 30 июня получить лицензию на ведение деятельности (позднее дедлайн перенесли на лето 2019 года). Для этого компании должны соответствовать вышеперечисленным правилам КРБСД.

Кроме того, p2p-платформы должны перестать формировать какие-либо резервы из фондов инвесторов, должны быть исключительно посредниками в отношениях между кредиторами и заемщиками и установить потолок на суммарную стоимость кредита 36% годовых (потолок суммарной стоимости кредита установил в 2015 году Верховный суд КНР).

Несвоевременный обвал

Западные СМИ пишут, что нынешний обвал на китайском рынке p2p-кредитования вызван как раз жесткими мерами со стороны регуляторов. С одной стороны, определенная логика в таких суждениях есть. Квазибанковский бизнес p2p по управлению активами потенциально мог принести гораздо больший доход, чем просто комиссионные за посреднические услуги. К тому же привлечение еще одного финансового посредника в лице депозитарного банка увеличивает транзакционные издержки, что также влияет на рентабельность p2p-бизнеса. Многие p2p-компании указывали на нечеткость требований и процедур для получения лицензий. Поэтому, как отмечает ряд СМИ, p2p-компаниям просто стало невыгодно работать, и они свернули свою деятельность.

Но дело в том, что первые правила КРБСД, как было сказано, опубликованы в конце 2016 года. Крайний срок исполнения этих правил, как и требований к лицензированию компаний, опубликованных Руководящей группой, не раз переносился. На данный момент переходный период продлен до июня 2019 года. Возникает вопрос: почему обвал на p2p-рынке произошел именно сейчас? По логике это должно было произойти или сразу, когда первые правила были опубликованы, или к истечению срока исполнения новых требований. А получилось так, что p2p-сектор рос вплоть до начала июня – за 12 месяцев, включая май, объем непогашенных займов вырос на 43%. А потом произошел резкий обвал.

Паника p2p-инвесторов началась в городе Ханчжоу. Именно там в апреле этого года власти ввели систему лотереи для покупки нового коммерческого жилья. Делалось это для того, чтобы сдуть пузырь на рынке недвижимости. Теми же соображениями руководствовались в свое время власти Пекина, когда вводили лотерею на получение регистрационных знаков на автомобили.

Но если в Пекине эксперимент удался и число новых машин на дорогах перестало расти гигантскими темпами, с недвижимостью в Ханчжоу получилось иначе. Во-первых, таким образом был искусственно разогрет спрос на вторичное жилье, на которое лотерея не распространялась. Во-вторых, для участия в лотерее нужно вносить аванс, который в случае розыгрыша особенно привлекательных лотов доходит до миллиона юаней. Таким образом,

людям срочно потребовались деньги, и они стали забирать свои инвестиции из p2p-платформ.

Если бы p2p-платформы работали как положено, просто связывая между собой кредиторов и заемщиков, то такой сценарий был бы невозможен: до истечения срока погашения задолженности кредитор не может требовать полный возврат средств. Но китайские p2p-платформы работали как квазибанки. Во многих была возможность досрочно вывести средства с потерей процентов.

Другой вопрос, что когда бегство инвесторов стало массовым, компании столкнулись с разрывом ликвидности и стали банкротиться. Первой закрылась крупнейшая p2p-платформа в Ханчжоу Shanlin Finance, не вернув $9 млрд инвесторам. Затем, уже в июне, обанкротились еще две старейшие p2p-платформы Ханчжоу – Tang Xiaoseng и Lian Bi finance.

Напряжения добавил глава КРБСД Го Шуцин (郭树清). Выступая на форуме Луцзяцзуй (陆家嘴论坛) 15 июня, он сказал, что инвесторы должны понимать связь высокой доходности с высоким уровнем риска. И предупредил, что если обещана доходность хотя бы 10%, то нужно быть готовым потерять все свои деньги. При этом большинство p2p-платформ как раз предлагали доходность от 10% и выше. Та же Tang Xiaoseng, например, обещала вкладчикам 12% годовых.

Видимо, тогда инвесторы отчетливо поняли, что государство никаких гарантий сохранности их вложений не дает. Поэтому после слов главы КРБСД даже те, кто не собирался в ближайшее время покупать недвижимость, бросились забирать нажитые непосильным трудом деньги. А были и те, кто, позарившись на высокую доходность p2p, вкладывался с большим кредитным плечом.

Люди набирали займов в микрофинансовых организациях, даже по кредитным картам, и вкладывались в p2p, рассчитывая заработать на спреде. Естественно, они запаниковали. Так и начались массовые банкротства p2p-компаний. И очень быстро эта волна захлестнула остальные регионы Китая. Еще больше осложнял ситуацию спад на фондовом рынке, куда многие p2p-платформы вкладывали деньги инвесторов.

30 лет перехода

Можно ли сказать, что китайский регулятор сам спровоцировал кризис, которого власти страны как раз пытались не допустить? Вряд ли. Волна банкротств началась еще до заявления Го Шуцина по гораздо более фундаментальным причинам, он лишь невольно ускорил неизбежное приближение коллапса. Регуляторы, наоборот, хотели как лучше: с одной стороны, разработать необходимое законодательство, а с другой – дать бизнесу время для перехода, чтобы избежать жесткой посадки.

Единственное, в чем просчитались власти, это в необходимости активного просвещения населения. Иначе как объяснить, что среди протестующих, которых задержали на подходе к офису КРБСД в Пекине, было много тех, кто вложил в единственную p2p-платформу все свои сбережения. Например, 47-летняя вдова, вложившая $550 тысяч, доставшиеся ей после смерти мужа. Теперь она осталась без сбережений, ей нечем оплачивать ребенку учебу. Или 28-летний работник

отеля, потерявший в p2p-платформе $66 тысяч, которые были предназначены для покупки жилья к свадьбе.

Теперь, понимая серьезность ситуации, власти пытаются разрешить кризис. На помощь призвали четыре государственные корпорации по управлению активами (AMCs), также известные как банки плохих долгов. Они в свое время были созданы, чтобы спасти финансовую систему страны, переходившей от плана к рынку.

Правда, как эти компании, набившие руку в реструктуризации задолженности и реализации залогов по кредитам, будут решать проблему p2p, непонятно. Ведь здесь никаких залогов и обеспечений не предусмотрено. Пекинское Управление по финансовой работе (北京市金融工作局) решилопредупреждать проблемы заранее и обязало все p2p-компании, работающие в местной юрисдикции, составить отчет о своей деятельности. Компании среди прочего должны будут сообщить о количестве активных пользователей, объем десяти крупнейших непогашенных займов и их отношение к общему объему займов, объем просроченных кредитов и так далее.

Эти меры подпитывают в китайском обществе патернализм, который как раз и вышел боком в случае с p2p-рынком. Государство, опасаясь социальных волнений, опять берет на себя и значительный контроль, и часть ответственности, которая по идее должна лежать на кредиторах и заемщиках. Похоже, что практика вмешательства государства в случае любого негативного события в сфере финансов привела к тому, что тридцатилетний переход Китая от плана к рынку пока еще так и не завершен. В сознании населения не укладывается, что доходность в пять раз выше, чем по депозитам, не может предлагаться просто так, и что, разумеется, государство не может давать гарантии по таким вложениям.

На самом деле даже полный крах p2p-рынка не был бы фатальным для финансовой системы страны: общий объем непогашенных займов p2p не превышает 1% от суммарного объема непогашенных банковских кредитов. Однако патерналистский общественный договор обязывает власти вмешаться и не допустить жесткой посадки.

Но проблема в том, что меры регулирования не могут быть эффективными, если в сознании населения не будет четкого понимания разницы между сбережением и инвестированием. Ведь помимо p2p есть и различные продукты по управлению активами, в том числе в банках, и инвестиционные продукты в страховых компаниях. При этом среднестатистический китаец считает, что это такие же безопасные вложения, как в банковские депозиты, просто под более высокие проценты.

Таким образом, спасая p2p-сектор, государство хоть и избегает небольших социальных волнений, но берет при этом на себя неограниченную ответственность. Люди будут по-прежнему ждать, что за любые их инвестиционные решения ответит государство. Но что делать в случае серьезного экономического кризиса? Как сдерживать десятки, если не сотни миллионов людей, которые пострадают в этом случае и будут ждать помощи от государства? Подобные шаги могут оказаться для Китая бомбой замедленного действия, которая рискует взорваться при наступлении серьезных финансовых проблем, например из-за последствий торговой войны с США».

3.3. Правовые аспекты P2P кредитования

3.3.1. Правовые аспекты P2P кредитования отражены в следующих статьях и обзорах:

- **КУЗНЕЦОВ В. А. Краудфандинг: актуальные вопросы регулирования. – Журнал «Деньги и кредит» n1 2017**
  http://www.cbr.ru/Content/Document/File/26473/kuznetcov_01_16.pdf
- **КАЗАЧЕНОК О.П. Взаимное (p2p) кредитование как современный инструмент альтернативного финансирования**
  https://cyberleninka.ru/article/n/vzaimnoe-p2p-kreditovanie-kak-sovremennyy-instrument-alternativnogo-finansirovaniya
- **ШАЙДУЛЛИНА В.К. Проблемы правового регулирования p2p-кредитования в Российской Федерации**
  https://cyberleninka.ru/article/n/problemy-pravovogo-regulirovaniya-p2p-kreditovaniya-v-rossiyskoy-federatsii
- **RBI опубликовал документ по пиринговому кредитованию. – ОБЗОР РЕГУЛИРОВАНИЯ ФИНАНСОВЫХ РЫНКОВ. n 1. 01.04.2016-15.05.2016. Банк России, 2016, С. 25-26**
  http://www.cbr.ru/StaticHtml/File/44019/review_280716.pdf

Последний из названных материалов представляет собой краткий обзор консультативного документа, опубликованного Резервным банком Индии и посвященного анализу существующих в мире моделей регулирования рынка P2P кредитования, а также аргументации в пользу и против введения регулирования этого вида кредитования. Материал содержит ссылку на полный текст документа RBI (на английском языке).

3.3.2. Законопроект "О привлечении инвестиций с использованием инвестиционных платформ" рассматривается в России с начала 2018 года, он направлен на регулирование платформ P2P кредитования. Материалы по его рассмотрению содержатся на официальном сайте Государственной Думы по адресу http://sozd.duma.gov.ru/bill/419090-7.

Здесь можно ознакомиться как с актуальным текстом законопроекта, так и с иными документами – пояснительной запиской к законопроекту, где содержится анализ возникающих проблем, а также отзывами Правительства на внесенные законодательные предложения. Все документы расположены в хронологическом порядке.

Ниже приводятся ссылки на материалы, содержащие разные мнения о законопроекте:

- **РБК – Россиянам запретят вкладываться по полной**
  https://www.rbc.ru/newspaper/2018/12/17/5c13a35e9a794757c75a2076

«Участие частных инвесторов в краудфандинговых проектах может быть ограничено

В России может быть введен лимит для частных вложений в различные проекты, в том числе криптоактивы, через краудфандинговые платформы, – максимум 600 тыс. руб. в год. Это должно снизить финансовые риски населения, считают в ЦБ.

Частные лица в России, не имеющие статуса квалифицированного инвестора, смогут инвестировать в проекты через краудфандинговые платформы не более 600 тыс. руб. в год,

при этом сумма вложений в один проект не должна превышать 100 тыс. руб. Такие требования содержатся в тексте законопроекта о регулировании краудфандинговых платформ (есть в распоряжении РБК), который готовится для рассмотрения Госдумой во втором чтении. Подлинность основных положений документа подтвердили два источника, знакомых с ходом его обсуждения.

В тексте законопроекта, принятого Госдумой весной 2018 года в первом чтении, говорилось, что лимит инвестиций будет устанавливаться нормативными актами Банка России. При этом сумма 600 тыс. руб. – это нижнее пороговое значение операций, подлежащих обязательному контролю со стороны Росфинмониторинга в рамках борьбы с отмыванием доходов.

Во втором чтении законопроект о краудфандинговых платформах, скорее всего, будет рассмотрен в январе 2019 года, рассказал РБК один из его авторов, глава комитета Госдумы по финансовым рынкам Анатолий Аксаков. «Данная версия законопроекта не ограничивает размер инвестиций в социальные или благотворительные проекты. Лимит установлен только для частных инвесторов, которые направляют денежные средства в коммерческие проекты», – уточнил он.

«Вложение инвестиций посредством краудфандинговых (инвестиционных) платформ является высокорискованным и может привести к потере всех инвестируемых денежных средств в полном объеме. С целью принятия неквалифицированными инвесторами таких рисков и вводится ограничение по объему инвестирования в течение одного года не более 600 тыс. руб.», – сообщили РБК в пресс-службе Банка России.

Рынок краудфандинга в России

Краудфандинговые платформы позволяют привлекать к финансированию различных проектов средства физических и юридических лиц. Они могут оформляться в виде займов, долей в уставном капитале или даже предусматривать нефинансовое вознаграждение за вложения (например, ужин со знаменитостью – инициатором проекта, приглашение на съемочную площадку, экземпляр изданной книги и т.д.). В рамках краудфандинга могут создаваться и ICO-проекты с выпуском криптоактивов.

По данным ЦБ, в 2017 году рынок краудфандинга в России удвоился, достигнув 11,2 млрд руб. Львиную долю на рынке занимает сегмент B2B (займы компаний или юрлицу юрлицом или ИП) с объемом 9,3 млрд руб. (плюс 81,5% к уровню 2016 года). Но самый динамичный сегмент – предоставление займов частными лицами юридическому лицу или индивидуальному предпринимателю, который вырос более чем в три раза, до 1,55 млрд руб. Средняя сумма сделки – около 300 тыс. руб. на одного человека, средняя сумма займа – чуть более 900 тыс. руб. в адрес одного юридического лица.

В сегменте краудинвестинга (привлечение денег юрлицом в обмен на долю в капитале, конвертируемые займы и т.д.) объемы в 10 раз меньше. В 2017 году они снизились на 52,4%, до 153,2 млн руб. Средняя сумма на финансирование одного проекта составила 8,1 млн руб., деньги за год привлекли 19 компаний.

Оценка охватывает не весь рынок: ЦБ составляет ее на основе совместного мониторинга с площадками, добровольно предоставляющими отчетность регулятору.

Текст уточненного ко второму чтению законопроекта предполагает, что операторы инвестиционных платформ (хозяйственные общества) вправе признать гражданина квалифицированным инвестором в соответствии с ФЗ «О рынке ценных бумаг», пояснили в ЦБ. В этом случае он будет иметь возможность инвестировать в течение одного года более 600 тыс. руб.

Гражданин может быть признан квалифицированным инвестором, если соответствует хотя бы одному из следующих критериев:

- наличие активов или определенных видов имущества на сумму не менее 6 млн руб.;
- опыт работы в организации из сферы ценных бумаг – не менее двух или трех лет в зависимости от статуса работодателя;
- операции с ценными бумагами за год с периодичностью не реже десяти за квартал, но не реже одной сделки в месяц при обороте не менее 6 млн руб.;
- наличие высшего экономического образования или специального финансового аттестата.

Из новой версии законопроекта исключены понятия «токен» и «смарт-контракты», но присутствует понятие «цифровые финансовые активы». Понятия «токены» и «смарт-контракты» были исключены и из законопроекта «О цифровых финансовых активах».

Законы о цифровых финансовых активах, о краудфандинговых платформах, а также поправки в Гражданский кодекс после принятия должны регулировать рынок криптоиндустрии в России.

Единицы крупных инвесторов

Физические лица чаще всего инвестируют по 5–10 тыс. руб. в один проект, рассказал РБК глава крупнейшей в России p2b-платформы Penenza.ru Дмитрий Пангин; при этом бывают случаи, когда за раз вкладывают 600 тыс. руб. – в основном это займы на участие в строительных тендерах или на исполнение контрактов.

Средний размер краудфандинговых инвестиций в проекты, связанные с творческой сферой (съемки фильмов, организация фестивалей), составляет, как правило, от 1 тыс. до 5 тыс. руб., сообщил РБК владелец краудфандинговой платформы Boomstarter Руслан Тугушев. «Случаев, когда сумма превышала бы предлагаемые ограничения (100 тыс. руб. на один проект, 600 тыс. руб. в целом за год), единицы», – говорит он. Столько же инвесторов, которые системно и в размерах, составляющих миллионы рублей, финансируют, к примеру, кинопроекты, добавил Тугушев.

Как считает владелец Boomstarter, если для краудфандинговых инвестиций все-таки потребуется быть квалифицированным инвестором, необходимо проработать упрощенную схему получения такого статуса. Такого же мнения придерживается и глава Penenza.ru. «Инвесторы с суммами свыше 600 тыс. руб. готовы получать статус квалифицированного инвестора. Главное, чтобы критерии были разумными и инфраструктура для получения такого статуса была готова, чтобы, например, инвесторам из регионов не приходилось ехать за тысячу километров для подтверждения статуса», – пояснил Пангин.

В Российской ассоциации криптоиндустрии и блокчейна (РАКИБ) установленную сумму ограничений считают сильно заниженной. По данным ассоциации, частный инвестор

вкладывает в ICO-проекты через краудфандинговые платформы около 1–3 млн руб. в год. Поэтому ассоциация предлагает установить лимит в размере до 2 млн руб.

Не «золотой стандарт»

Целью предлагаемых поправок является ограничение рисков для индивидуальных инвесторов, полагает старший юрист Herbert Smith Freehills Денис Морозов. «Для регулятора «золотым стандартом» является вклад в банке, так как возврат вкладов до определенной суммы гарантирован системой страхования вкладов. Любые менее надежные инструменты вызывают закономерное опасение, так как часто неквалифицированные инвесторы не способны оценить перспективы возврата своих средств и подвергают их чрезмерному и неосознанному риску», – поясняет он. «Это будет абсолютно закономерное ограничение граждан в использовании собственных средств», – считает юрист.

В России неквалифицированные инвесторы не могут приобретать «ценные бумаги, предназначенные для квалифицированных инвесторов», например, паи некоторых инвестиционных фондов или акции иностранных эмитентов, не допущенных к публичному размещению или обращению в России, напоминает Морозов.

Партнер компании НАФКО Ирина Мостовая считает, что для ЦБ данный законопроект – шаг к повышению контроля над рынком P2P-кредитования, который до сих пор является одним из наименее зарегулированных. Это в первую очередь борьба с транзакциями, направленными на вывод средств из экономики, в том числе за счет инвестиций в зарубежные проекты, полагает она.

Опыт других стран

Минимальный порог для участия в рискованных финансовых операциях существует в большинстве юрисдикций мира, в том числе в США, Японии и во всех странах Европейского союза, рассказал руководитель блокчейн-интегратора Sputnik DLT Артем Толкачев.

По словам основателя краудфандинговой блокчейн-платформы BitRussia Ивана Родионова, вводя лимит на инвестиции со стороны неквалифицированных инвесторов, Россия ориентируется на опыт Китая, где ограничения были введены в связи с ростом мошенничества. «В Китае краудфинансовый рынок рос невероятными темпами в 2007–2015 годах, но обвалился в 2016-м. Самая крупная площадка Ezubao оказалась финансовой пирамидой, она увела $7,3 млрд у 900 тыс. инвесторов», – отметил Родионов.

В сентябре 2017 года власти Китая запретили проведение ICO в стране, посчитав, что 90% подобных размещений являются мошенническими, напомнил он. На данный момент для физлиц в Китае установлен лимит на предоставляемый заем в размере суммы, эквивалентной 1,95 млн руб. на одной площадке, долг по всем площадкам не может превышать 9,7 млн руб. Для юрлиц лимиты составляют суммы, эквивалентные 9,7 млн и 48,5 млн руб. соответственно».

- **Хайтек + – Госдума ограничит инвестиции россиян в криптовалюты и ИТ-проекты https://hightech.plus/2018/12/17/gosduma-ogranichit-investicii-rossiyan-v-kriptovalyuti-i-it-proekti**

«Депутаты намерены ввести лимит для частных лиц на финансирование проектов через краудфандинговые платформы – не более 600 тыс. рублей в год и не более 100 тыс.

в один проект. В Центробанке заявляют, что заботятся о сохранности денег неквалифицированных инвесторов.

В Госдуме готовится ко второму чтению законопроект о краудфандинговых платформах – популярном способе софинансирования проектов в сфере высоких технологий. В Центробанке хотят ограничить такой вид инвестиционной активности россиян: вкладывать можно будет не более 100 тыс. рублей в один проект и не более 600 тыс. рублей за год.

Проект закона о краудфандинге был принят Госдумой в первом чтении весной 2018 года. В тексте говорилось, что лимит инвестиций будет устанавливаться нормативными актами Банка России. Теперь Центробанк озвучил свою позицию.

«Вложение инвестиций посредством краудфандинговых (инвестиционных) платформ является высокорискованным и может привести к потере всех инвестируемых денежных средств в полном объеме», – заявили в пресс-службе ЦБ агентству РБК.

РБК обращает внимание, что годовой порог в 600 тыс. рублей – это сумма, по превышении которой операциями интересуется Росфинмониторинг, проверяя их на отмывание денег.

Юристы считают, что инициатива ЦБ – шаг к повышению контроля за рынком P2P-кредитования, который до сих пор является одним из наименее зарегулированных. Это в первую очередь борьба с транзакциями, направленными на вывод капиталов из страны, в том числе за счет инвестиций в зарубежные проекты.

До вмешательства ЦБ рынок краудфандинга в России бурно развивается. В 2017 году он удвоился, его объем превысил 11 млрд рублей.

Самый динамичный сегмент – предоставление займов частными лицами юридическому лицу или индивидуальному предпринимателю, который вырос более чем в три раза, до 1,55 млрд руб.

Новое регулирование будет касаться и «цифровых финансовых активов», то есть ICO и криптовалют.

Юристы указывают, что участие населения в высокорискованных финансовых операциях ограничено в большинстве стран, в том числе в США, Японии и Евросоюзе. В Китае краудфандинг ограничили после краха площадки Ezubao, которая оказалась финансовой пирамидой и увела у своих 900 тыс. инвесторов $7,3 млрд. Помимо прочего, в Китае истребили криптовалюты, запретили ICO и блокируют доступ к сайтам о криптовалютах».

4. Кейс «Страхование вкладов»

При работе над этим кейсом обратите внимание, что согласно Федеральному закону "О страховании вкладов физических лиц в банках Российской Федерации" вкладчики имеют право получать возмещение по вкладам только в порядке, установленном этим законом (статья 7).

Поэтому при наступлении страхового случая и несогласии вкладчика с рассчитанным банком размером вклада (или еще хуже - отсутствии указания на вклад в банковских документах) вкладчику требуется представить в Агентство по страхованию вкладов дополнительные документы, подтверждающие обоснованность его требований (статьи 10, 12).

Перечень таких документов определен Порядком выплаты возмещения по вкладам, утвержденным решением Правления Агентства от 3 августа 2006 г. (протокол № 46) (последняя редакция утверждена решением Правления Агентства от 6 ноября 2018 г. (протокол № 127) (текст можно скачать по ссылке http://www.asv.org.ru/documents_analytik/documents/search/551987/).

Согласно Разделу VIII Порядка "Урегулирование разногласий о размере возмещения", для подтверждения обоснованности требований, связанных с выплатой возмещения, заявитель представляет дополнительные документы (их оригиналы или надлежащим образом заверенные копии):

1) договоры банковского вклада и (или) банковского счета, сберегательные книжки, сберегательные сертификаты, на основании которых возникло право требования к банку;
2) судебные решения, а также исполнительные листы и (или) постановления судебного пристава-исполнителя о возбуждении исполнительного производства, подтверждающие наличие обязательств банка перед вкладчиком по договорам банковского вклада и (или) банковского счета;
3) приходные ордера и выписки по счетам, подтверждающим размещение вкладчиком денежных средств во вклад, подлежащий страхованию в соответствии
с Федеральным законом № 177-ФЗ;
4) иные документы, подтверждающие обоснованность требований заявителя.

4.1. Выступления экспертов, консультации, рекомендации

4.1.1. Мнения профессиональных участников рынка о рисках онлайн-вкладов

- **РИА НОВОСТИ – Глава АСВ видит риски в возмещении вкладов в онлайн-банках в будущем**
  https://ria.ru/20170713/1498468403.html

«Агентство по страхованию вкладов (АСВ), скорее всего, не сможет возмещать вклады клиентам онлайн-банков в РФ в будущем по скрин-шотам в мобильных телефонах без наличия бумажной выписки, поэтому необходимо уточнять законодательство, заявил глава Агентства по страхованию вкладов (АСВ) Юрий Исаев на Международном финансовом конгрессе.

Юрий Исаев уточнил, что имеет в виду не все онлайн-банки, а недобросовестных игроков, которые не дают возможности клиенту получить подтверждение отношений между клиентом и банком в бумажном виде, отметив, что у крупнейших российских онлайн-игроков эта опция есть и что все первичные документы у добросовестных онлайн-банков с лицензией ЦБ есть в первичном виде.

«Речь идет не обо всех онлайн-банках, а о недобросовестных игроках, мошенниках, которые намеренно не дают возможности клиенту получить подтверждение договорных отношений в бумажном виде», – отметил он.

«Меня сильно, несмотря на то что эта тема модная, пугает онлайн-банк. Не в том смысле, что я ретроград и хочу все на бумаге видеть. Абсолютно нет, меня беспокоит то, что если не дай бог встанет какой-то крупный онлайн-банк, в котором у нас не будет никакой «первички» (документов-подтверждений по вкладам – ред.), то нам будет реально сложно», – сказал Исаев.

«Мы под скрин-шотом с мобильных устройств с большой долей вероятности выплачивать сразу не сможем, пока у нас нет никакой законодательной защиты в этом плане», – заявил он.

Сейчас АСВ пытается найти хоть какие-то бумажные документы, подтверждающие вклады в рухнувших банках, отметил он. «Если у нас случится такой онлайн-disaster (крах онлайн-банка – ред.), с чем мы будем сравнивать, если в самом банке умудряются тоже уронить базу. Этот случай нам надо заранее осмыслить и описать, хотя бы в какой-то период – раз в квартал – вкладчик должен получить на бумаге выписку в онлайн-банке, чтобы она у него хранилась», – подчеркнул Исаев.

«Нет выписки, нет базы данных, есть скрин-шот на телефоне – мы в патовой ситуации. Мы как АСВ должны всегда сравнивать источник информации, если у нас один источник информации – мы в тупике. Если у нас два источника информации – мы с большой долей вероятности решим наши задачи. Если у нас три источника информации, должно быть по закону, тогда мы сейчас всегда выплачиваем в течение двух недель. Поэтому нужно подумать о том, что нас ждёт в перспективе», – призвал он».

- **Финансист – Вклады онлайн**
  https://finansist-kras.ru/consultant/competence/vklady-onlajn/

«Экономить время, выбирать удобный сервис – тренд, диктуемый временем и технологиями. Сегодня продвинутые пользователи открывают банковские вклады в режиме онлайн, минуя очереди в отделениях. И это не только удобно, но, зачастую, ещё и выгодно.

Портал «Финансист» в очередной раз актуализировал информацию – в каком банке и на каких условиях можно открыть вклад через интернет.

ВАЖНО! Необходимое условие для открытия вклада онлайн: уже иметь в данном банке счёт – тогда банк может опознать клиента, не вступая в противоречия с банковским законодательством.
Банки Красноярска, в которых можно открыть вклады онлайн:

Итак, Красноярцы могут открыть вклад онлайн в следующих банках: Авангард, АТБ, АК Барс Банк, Акцепт, Альфа-Банк, банк Интеза, БИНБАНК, БКС

Премьер, Восточный банк, ВТБ, Дальневосточный банк, Кредит Европа Банк, банк Левобережный, МТС-Банк, Открытие, ОТП Банк, Почта Банк, Промсвязьбанк, Райффайзенбанк, Ренессанс Кредит, Росбанк, Росгосстрах банк, Россельхозбанк, Русский стандарт, Сбербанк, Связь-Банк, СКБ-Банк, Совкомбанк, Уралсиб, Хоум кредит, Экспобанк, ЮниКредитбанк.

Также в большинстве этих банков можно пополнять вклад, открытый дистанционно (а иногда и все вклады), таким же образом.

Все ли вклады в банке можно открыть через интернет?

Примерно в половине случаев у банков есть ограничения по выбору вклада из действующей линейки. Другими словами, любой вклад, из предлагаемых банков в режиме «офлайн», открыть «онлайн» удастся не всегда. Политика банков в этом вопросе весьма разнообразна, так что стоит уточнять детали в индивидуальном порядке. Например, в банке ВТБ такая возможность предусмотрена для всей линейки, а в Сбербанке в режиме онлайн открываются только несколько вкладов.

Светлана Туровец, заместитель управляющего Красноярским отделением Сбербанка даёт подробную инструкцию: «Сбербанк предлагает 3 онлайн вклада:

- Сохраняй онлайн» (вклад без возможности пополнения, снятия суммы);
- «Пополняй онлайн» (допускается пополнение депозита на 1 000 рублей и более);
- «Управляй онлайн» (вклад можно пополнять, снимать его часть).

Для их открытия человек должен быть клиентом банка и иметь доступ в Сбербанк Онлайн. Необходимо войти в интернет-банк, перейти в раздел «Вклады и счета», «Открытие вклада» и заполнить все поля: выбрать вид вклада, валюту, указать счет, с которого будет списаны деньги на вклад, ознакомиться с условиями. Если все правильно – отмечаете согласие с условиями и подтверждаете заявление на открытие вклада. Успешная операция переводится в статус «исполнено», что незамедлительно отражается на экране. На этой же странице вы увидите реквизиты открытого счета. Убедиться в том, что новый вклад действительно открыт, можно перейдя в раздел «Вклады и счета» системы Сбербанк Онлайн. Там же можно повторно ознакомиться с реквизитами и подробной информацией об условиях открытого вклада.

Сделать это можно не только в web-версии, но в мобильном приложении Сбербанк Онлайн, установленном на гаджете. Подтверждением открытия вклада будет договор, который будет направлен вам на электронную почту. Договор банковского вклада, открытого в Сбербанк Онлайн, можно распечатать в личном кабинете в разделе «История операций» самостоятельно, либо получить, обратившись в любой офис банка. Преимуществом дистанционного банковского вклада является возможность осуществления операций по ним практически круглосуточно – через интернет-банк. И, конечно, у онлайн вкладов есть приятный бонус – ставки по ним, как правило, немного выше в сравнении с обычными вкладами. Например, ставка по вкладу «Сохраняй» в Сбербанке составляет до 4,2% годовых, а по вкладу «Сохраняй Онлайн» – уже 4,45%, без учета капитализации процентов».

Обратите внимание, довольно часто минимальная сумма для открытия вклада через интернет существенно ниже, чем аналогичный показатель для этого продукта при открытии в отделении, что, безусловно, тоже есть большой плюс в копилку новых технологий.

Александр Парамонов, директор Азиатско-Тихоокеанского банка по розничному бизнесу: «Эта услуга все больше набирает популярность среди клиентов АТБ, так как, в первую очередь, это очень удобно: нужно провести всего несколько действий за компьютером или в телефоне, буквально не выходя из дома. Во-вторых, по вкладам Онлайн клиенты получают повышенный доход. В-третьих, помимо вкладов в режим онлайн можно совершать множество других операций: платежи и переводы, переводы с карты на карту, оплата налогов и штрафов ГИБДД, настройка шаблонов и автоплатежей и многое другое.

Процентные ставки по вкладам Онлайн выше на 0,2 п.п., чем при открытии аналогичных вкладов в офисах банка. На текущий момент открыть вклад можно только в рублях, но наш банк уже работает над тем, чтобы была возможность открывать вклады и в других валютах (доллары США, евро, китайский юань). Онлайн можно открыть вклады сроком 182/367/731/1098 дней. В офисах АТБ есть возможность открыть вклады и на более короткие сроки (31 день, 92 дня). В остальном все условия по вкладам Онлайн и в офисах АТБ абсолютно идентичны.

Для открытия Онлайн-вклада в Азиатско-Тихоокеанском банке необходимо иметь только банковскую карту АТБ и доступный остаток, позволяющий это сделать. Онлайн можно открыть базовые вклады, удовлетворяющие трем основным потребностям клиентов: накопить/сохранить/управлять».

Кроме того, некоторые банки даже запускают специальные вклады для интернет-банка (к примеру, банк Авангард, АТБ, Банк Интеза, Кредит Европа банк, Русский стандарт, Сбербанк, СКБ-банк, Хоум кредит, Экспобанк и ЮниКредитбанк), а банки АК Барс, Банк ВТБ, Банк Открытие, БИНБАНК, БКС Премьер, Восточный банк, Почта банк, Промсвязьбанк, Ренессанс кредит, Росбанк, Россельхозбанк, Совкомбанк, Уралсиб предлагают повышенные ставки. Плюсом идёт разброс 0,05 – 1% годовых к ставке по продукту – как говорится, мелочь, а приятно.

Антон Шевнин, региональный директор ОО «Красноярский» Сибирского филиала ПАО «Промсвязьбанк»: «У нас есть надбавки для клиентов, которые открывают вклад в интернет-банке, к ставке прибавляется от 0, 1 до 0,25%. Таким образом, клиент не только экономит время, но и получает большую доходность по депозиту. В дистанционных каналах ПСБ есть калькулятор вкладов, который сможет подобрать самое выгодное предложение для клиента. Все вклады, за исключением предложения «Моя стратегия», можно открыть онлайн.

Конечно, открыть вклад в интернет - или мобильном банке могут те клиенты, которые ранее пользовались продуктами ПСБ. Клиенту нужно зайти в приложение или ИБ, сделать несколько кликов и вклад будет открыт.
Вклад до 1 миллиона рублей можно закрыть в интернет- или мобильном банке и снять деньги в банкомате Промсвязьбанка. Для сумм более 1 миллион рублей необходимо личное обращение в банк».

Евгения Кравцова, директор филиала ПАО «Дальневосточный банк» в г. Красноярск: «Вклады онлайн в Дальневосточном банке входят в число наиболее востребованных услуг. Управлять своими сбережениями в реальном времени особенно удобно для тех, кто в силу занятости не может посетить офис банка.

Открыть вклад онлайн в Дальневосточном банке очень просто – нужно воспользоваться системой «Интернет-офис», которая дает возможность управлять личным вкладным счетом, находясь в любой точке планеты, через Интернет. Подключить услугу «Интернет-офис» можно, являясь держателем пластиковой карты Дальневосточного банка, в транзакционных терминалах, банкоматах Дальневосточного банка или через круглосуточный контакт-центр.

Открыть в реальном времени можно наиболее востребованные вклады: «Быстрый доход», «Высокий доход», «Депозит + расходные операции», «Депозит + досрочное расторжение». Наши вклады ориентированы на клиентов с различными потребностями и уровнем дохода. Вклады в ПАО «Дальневосточный банк» застрахованы государством. При открытии вклада в Дальневосточном банке сумма вклада и ставка по нему не зависят от способа открытия вклада. При этом, вклад, открытый онлайн, может быть пролонгирован автоматически, что очень удобно, клиенту не нужно идти в отделение банка, чтобы открыть новый вклад.

Преимущества размещения средств во вклады онлайн давно оценили клиенты банка. Кроме открытия, пролонгирования и закрытия в Интернет-офисе предусмотрено пополнение вкладов. К примеру, получая заработную плату на свою пластиковую карту, можно пополнить вклад на нужную сумму, не отходя от компьютера. Кроме того, можно пополнять и депозитные счета в других банках».

В пресс-службе банка ВТБ поясняют: «Ставки по онлайн-вкладам всегда выше, чем по вкладам, открываемым в офисе банка. Он-лайн вклады позволяют самостоятельно, с помощью конструктора выбрать наиболее подходящий тип вклада, исходя из суммы, срока, возможной капитализации начисляемых процентов, пополнения и снятия средств на период действия вклада. Открыть онлайн-вклад в нашем банке можно в личном кабинете на сайте или в мобильном приложении. Получить доступ для входа в личный кабинет можно в офисе банка. Далее все операции в интернет-банке ВТБ-Онлайн клиент может совершать самостоятельно: гасить кредиты, переводить средства с карты на карту, оплачивать различные сервисы и услуги, а также открывать различные виды вкладов и накопительные счета. Вклады могут быть как рублевыми, так и в иностранной валюте. Средства с вклада вы можете снять как после истечения его срока действия, так и самостоятельно закрыть вклад досрочно, согласно действующим по вашему вкладу условиям. Все условия по каждому из вкладов указаны в личном кабинете в ВТБ-Онлайн. Все вклады до 1,4 миллиона рублей застрахованы в АСВ».

Технические подробности и другие нюансы при открытии вклада через интернет

Электронная версия договора доступна клиенту в интернет-банке. Всё-таки рекомендуем вкладчику, после оформления депозита через интернет, найти потом возможность зайти в офис банка и таки получить бумажный вариант договора вклада. Во избежание гипотетических проблем с Агентством Страхования Вкладов (да, вклады, сделанные в онлайне, тоже застрахованы на общих условиях).

Сама процедура открытия депозита немногим отличается от обычной операции в интернет-банкинге. Клиент заполняет заявление на открытие вклада и одновременно передает поручение о списании с одного или нескольких его банковских счетов в размере суммы вклада. Подтверждением операции в настоящее время является использование

клиентом разового ключа или электронно-цифровой подписи. В случае акцепта банком заявления клиента он предоставляет клиенту подтверждение об открытии вклада.

Андрей Покидышев, региональный директор операционного офиса «Центральный» Филиала ООО «Экспобанк» в г. Новосибирске: «При открытии вклада с использованием Интернет-банк «Expo-online» Заявление на открытие вклада передается в банк в форме электронного документа, подписанного электронной подписью вкладчика. Экземпляр оригинала заявления на открытие вклада, с соответствующей отметкой банка доступен вкладчику в личном кабинете Интернет-банке «EXPO-online» в разделе «Заявления». Подтверждением заключения договора является распечатанное, из личного кабинета Интернет-банка, заявление и этого достаточно. При необходимости наличия справки о размещении денежных средств во вклад или получения заявления на бумажном носителе с отметкой банка о его равнозначности электронному документу, необходимо обратиться в банк, предъявив документ, удостоверяющий личность».

Александр Парамонов, Азиатско-Тихоокеанский банк: «После проделанной операции формируется чек, который подтверждает открытие вклада, и вкладчик может его сохранить/распечатать. В офисе АТБ клиент в любое время может получить оригинал договора вклада».

Антон Шевнин, Промсвязьбанк: «При открытии вклада в личном кабинете формируется пакет документов в формате pdf с факсимильной подписью, которые можно распечатать и в случае необходимости предъявлять в качестве подтверждения открытия депозита. Так же получить документы, подтверждающие открытие депозита, можно в любом офисе банка. Пакет документов состоит из заявления и платежного поручения».

Закрыть вклад, открытый посредством интернет-банка, можно с использованием этого же канала, переведя средства со своего вклада на свои счета.

Евгения Кравцова, Дальневосточный банк: «По истечению срока действия договора денежные средства возвращаются на счет, с которого они были переведены на вклад. Досрочное закрытие вклада в ПАО «Дальневосточный банк» можно осуществить в офисе банка, либо онлайн через систему «Интернет-офис». Если вклад закрывается в офисе банка, то получить денежные средства клиент может наличными или они будут переведены на указанный клиентом счет. Если вклад закрывается через Интернет-офис, то денежные средства будут переведены на указанный клиентом счет».

Андрей Покидышев, Экспобанк: «В дату окончания срока вклада закрытие вклада в интернет-банке осуществляется простым безналичным переводом денежных средств со вклада на счет в банке или на счет в другом банке по реквизитам. В случае необходимости получения вклада наличными денежными средствами или для закрытия вклада досрочно требуется обратиться в отделение банка».

Удобство сервиса открытия и пролонгации вкладов, а также постоянное совершенствование прикладных приложений приводит к тому, что доля вкладов, открываемых в режиме онлайн, постоянно растёт, констатируют банки.

Григорий Иванюк, начальник управления розничного бизнеса банка «Левобережный» (ПАО): «Для того, чтобы открыть вклад онлайн в нашем банке, достаточно подключить услугу Интернет Банк (ИБ), после чего в личном кабинете будет доступна операция «открытие вклада». Список доступных вкладов клиент видит в Интернет

Банке) и может выбрать любой из предложенных. У открытия вклада в режиме онлайн, на наш взгляд, недостатков нет, из плюсов можно отметить экономию времени и более высокий процент по вкладу. И клиенты активно пользуются этой возможностью. Так как все клиенты ценят время, а вклад онлайн – это удобный способ без посещения офиса банка разместить денежные средства под высокий процент».

Светлана Туровец, Сбербанк: «Каждый четвертый вклад в банке сейчас открывается дистанционно. Это и неудивительно, ведь онлайн-банкинг – давно не прерогатива особо продвинутых клиентов, а реальность, которая становится все более доступной самому широкому кругу потребителей банковских услуг».

Андрей Покидышев, Экспобанк: «Онлайн вклады набирают огромную популярность среди клиентов, так как позволяют экономить личное время. Оформить вклад с повышенной ставкой (до 0,2% в рублях) возможно в любое время суток, в выходные и праздничные дни без посещения банка. На текущий момент, данная опция доступна только для вкладов «Онлайн Лидер» и «Онлайн Лидер актив». Это очень удобно, особенно с учетом занятости населения и пробок. Онлайн-вклад доступен только действующим клиентам, у которых подключен сервис Интернет-банк «Expo-online», поэтому новым клиентам посетить отделение всё же придется, и это скорее не минус, а возможность стать клиентом банка и удобство использования услуг в дальнейшем».

- **Sravni.ru – Опасно ли открывать вклады онлайн?**
  https://www.sravni.ru/q/opasno-li-otkryvat-vklady-onlajn-15027/

«Что происходит с забалансовыми вкладчиками с учётом того, что у них нет на руках документов в бумажном виде, которые бы подтверждали открытие вклада – договора, выписок по счёту и др?

Диана Маклозян

В настоящее время большинство банков предоставляют онлайн-услугу по открытию вкладов. Для открытия такого вклада требуется всего лишь выбрать вид вклада (порядок пополнения, снятия, проценты по вкладу), а также согласиться с условиями вклада, которые предлагает банк. Открытие таких вкладов совершенно безопасно, даже при отсутствии документов на руках можно будет подтвердить открытие и движение средств по этому вкладу выписками по счетам.

С забалансовыми вкладчиками совсем другая история, ими могут стать и те, кто открывал свои банковские счета в офисах и имеет на руках все документы, подтверждающие наличие такого счёта. Так, при открытии счетов банки фальсифицируют данные о клиентских депозитах, искажая их в своем внутреннем бухгалтерском балансе с помощью различных мошеннических схем. Банки рассчитывают на то, что при закрытии банковского счёта вкладчиком ему будет возвращена вся сумма депозита, однако при банкротстве банки не всегда успевают привести бухгалтерский баланс в порядок, и искажённые данные передаются в АСВ. Именно в таких случаях часть денежных средств некоторых вкладчиков оказывается за пределами официального баланса банка и не входит в реестр вкладов АСВ. Таким образом, вкладчикам приходится доказывать точную сумму денежных средств, которая была у них на счетах, подтверждая всё это сохраненными выписками и иными документами, подтверждающими операции.

Надежда Куликова

На мой взгляд, открытие вклада самостоятельно в online-канале (через интернет-банк или мобильный банк), наоборот, более надёжно, чем в офисе. При использовании интернет-банка (мобильного банка) вы самостоятельно осуществляете процедуру открытия вклада, которая проводится автоматизированно (без участия операционного работника банка). Получается, что счёт сразу открывается в банковской системе, деньги переводятся на открытый вами счёт. Вы это делаете всё сами и без посредников.

Если вас смущает отсутствие бумажного договора, то это вовсе не проблема. После открытия вклада через интернет-банк (мобильный банк) вы всегда можете подойти в офис банка и попросить распечатать ваш экземпляр договора.

Для ещё большей уверенности в том, что ваш вклад корректно оформлен (как в офисе, так и через дистанционный канал), вы можете запросить в офисе банка выписку из реестра АСВ. Банки должны формировать данный документ на момент обращения клиента. Выписка из реестра АСВ формируется по конкретному клиенту с указанием всех его счетов и остатков на них на дату формирования выписки, а также номера вкладчика в реестре АСВ. При этом речь идет о корректно работающем банке (без наступления какого-либо страхового случая).

Вадим Башир-Заде

Хотя большинство банков предоставляет возможность открытия вклада онлайн, в этой сфере сохраняется риск мошенничества. Но связан этот риск в первую очередь с операциями по вкладу, совершаемыми по интернет-каналам. Проблемой может стать как вредоносная программа, перехватывающая конфиденциальную информацию, так и обычное воровство данных. Кроме того, ни один банк не застрахован от технического сбоя. В результате такого сбоя база данных с информацией о вкладе и о вкладчике может измениться или вовсе исчезнуть.

Отсутствие бумажных документов об операциях по таким вкладам не является существенной угрозой для вкладчика. Сейчас почти во всех банках установлен порядок, согласно которому используется бумажная документация, дублирующая все электронные записи по счёту Реестры движений по счетам ежедневно печатаются, заверяются надлежащим образом и сдаются на хранение.

То есть при наступлении страхового случая все сведения об онлайн-вкладе клиента и движениях по такому вкладу будут поступать из банка в АСВ как в электронном, так и в бумажном виде. Поэтому клиенту при обращении в АСВ будет достаточно лишь предъявить документ, удостоверяющий личность. Договор об открытии вклада и выписки со счёта в бумажном виде клиенту в этом случае можно не предоставлять».

- **Вклады в банках Москвы – Вклады через интернет-банк – насколько это надежно?**
  http://www.vkladvbanke.ru/sovety/vklad-cherez-internet-bank.html

«На волне роста количества банков, предлагающих частным лицам открыть вклад дистанционно, все большее число банковских клиентов интересуется, насколько виртуальные договоры надежны и безопасны в отношении средств вкладчиков. В этой статье мы не будем анализировать уровень информационной и технической безопасности обмена данными через электронные каналы связи. Посмотрим на вопрос со стороны

легитимности договора банковского вклада, имеющего лишь виртуальные подписи заинтересованных сторон.

Нормативная база

Сразу заверим обеспокоенных вкладчиков – электронные подписи и документы вполне узаконены российским законодательством. Регламентирующих нормативных актов множество. Приведем в пример лишь основные: статьи 434, 428, 836 Гражданского кодекса РФ, Закон от 27 июля 2006г. № 149- ФЗ «Об информации, информационных технологиях и о защите информации», Закон от 02 декабря 1990г. N 395- 1 «О банках и банковской деятельности», Закон №177-ФЗ от 23 декабря 2003г. «О страховании вкладов физических лиц в банках Российской Федерации», Закон от 06 апреля 201г. № 63-ФЗ «Об электронной подписи» (вступивший в действие в июле 2012г. и заменивший старый Закон № 1-ФЗ от 10 января 2002г.), Закон от 7 февраля 1992г. N 2300-1 «О защите прав потребителей», Положение от 26 марта 2007г. № 302-П «О правилах ведения бухгалтерского учета в банках» и т.д.

В свою очередь сами кредитные учреждения прописывают необходимые юридические обоснования во внутренних Правилах, регламентирующих порядок документооборота. Наличие Правил контролирует надзорный орган от государства – Банк России. К сожалению, Центробанк не оценивает правовые аспекты юридических терминов в содержании.

Удобно и выгодно

Приглашения открыть вклад в онлайн-системе начали появляться относительно недавно, несмотря на многолетнее существование интернет-банкинга. Пока в Москве такой сервис рекламируют чуть больше двух десятков кредитных учреждения с банковской лицензией. Хотя, конечно, с ростом популярности услуги на рынке будет увеличиваться и количество предложений.

Надо отметить, что сама система дистанционного доступа к банковскому счету появилась у российских клиентов еще в конце прошлого века. Сначала интернет-банкинг был привилегией юридических лиц. Потом и физические лица получили возможность управлять финансами в онлайн режиме. Но открывать депозит через интернет пока могут клиенты далеко немногих банков. Сегодня довольно быстро приумножается число разнообразных дистанционных услуг для граждан от «банк-клиента», «интернет-банка» и «мобильного банка» до «электронных кошельков» платежных систем.

Несомненно, сервис онлайн очень удобен для всех. При этом банк сокращает накладные расходы на прием и обслуживание клиентов в офисах, параллельно решая вопрос о хранении бумажного архива. Сами вкладчики экономят время на посещение кредитных учреждений, ожидание в очередях и общение с банковскими служащими в офлайн-режиме. Выгода очевидна – одни наращивают клиентскую базу и привлеченные денежные ресурсы. Другие получают удобную возможность быстрого управления своими средствами 7 дней в неделю и 24 часа в сутки, а, следовательно, и дополнительное время, чтобы еще больше зарабатывать и тратить эти денег.

Риски и как их снижать

Но, говоря об избавлении от лишних бумаг, удобстве и увеличении скорости получения услуг, нужно помнить об определенных рисках, сопутствующих электронному документообороту: например, масштабный сбой электропитания, компьютерный вирус или банкротство банка. В этом смысле можно посоветовать более серьёзно подходить к выбору депозитарного института для личных сбережений, особенно планируя использовать технически сложные банковские продукты. Только грамотная и профессиональная организация процесса внутри банка позволит сохранить денежные средства клиентов.

Расскажем, как в самих кредитных учреждениях решается проблема страхования от подобных рисков. Не секрет, что все электронные транзакции от бухгалтерских проводок, простых операций до ЭЦП на документах хранятся на компьютерном сервере. В каждом банке должны существовать несколько серверов, в том числе запасных, куда вся информация копируется порой по несколько раз в день. Кроме того, существуют организационные регламенты, предписывающие порядок действия сотрудников на случай сбоя программного обеспечения. В этих обстоятельствах банковские служащие должны пользоваться бумажной документацией, обязательно дублирующей все электронные записи по счетам клиентов. Реестры движений по бухгалтерским счетам ежедневно печатаются, подписываются руководством и сдаются в архив.

Внутренний и внешний аудит периодически проверяет соблюдение правильного документооборота.

При наступлении страхового случая банкротства актуальные сведения о клиентских операциях должны поступать в государственное агентство по страхованию вкладов и в электронном, и в бумажном виде. На основании такой информации составляется реестр вкладчиков, которые могут рассчитывать на возмещение по банковским счетам – депозитным, текущим или карточным. Поэтому для обращения в АСВ достаточно будет предъявить документ, удостоверяющий личность без бумажного договора банковского вклада или счета.

Напомним, что по действующему сегодня законодательству страхованию в АСВ не подлежат вклады в драгоценных металлах и инвестиционные вложения в паи или ценные бумаги с повышенной доходностью. Последние часто входят в состав структурных продуктов, частью которых являются и банковские депозиты. О таких наш сайт уже писал ранее. Поэтому государственному страхованию подлежат не все депозитные продукты.

Учитывая субъективные факторы ведения банковского дела, думаем, надежнее было бы иметь на руках бумажный оригинал подписанного договора с юридическим лицом, который пригодится на случай обращения с жалобой в Центральный банк или в суд. Хотя сейчас и эти организации принимают в качестве доказательств электронные документы.

Но многие ли частные лица умело хранят их в своем компьютере с надлежащей ЭЦП? Ведь судебные органы, прежде всего, будут запрашивать подтверждение на цифровом или бумажном носителе у обеих сторон. К тому же некоторые юристы говорят о спорности иных терминов и положений, которые применяют банки в своих отношениях с потребителями их услуг. Нелишним будет напомнить о различиях в технологиях систем «Банк-клиент» и «Интернет-банкинг». Только первая подразумевает установку на компьютере специального программного обеспечения, которое хранит информацию ее владельца. Вторая система не держит в памяти клиентской машины ничего.

Практика документального оформления

Посмотрим, какие условия открытия вкладов через интернет прописаны в документах крупнейших российских банков. Альфа-Банк заключает с физическими лицами Договор комплексного обслуживания, состоящий из 73-х листов. В нем предусмотрены варианты открытия депозитов без дополнительного заключения договора вклада. Подтверждением двустороннего соглашения является заявление от гражданина о присоединении к общему Договору, которое может быть отправлено с помощью ЭЦП через интернет. Банк обязывает клиента знакомиться каждые 5 дней с возможными обновлениями в правилах обслуживания, но оставляет за ним право не забирать свой экземпляр оригинала документа с «живой» подписью руководителя.

В Промсвязьбанке несколько иная технология, впрочем, очень похожая на аналогичные в других учреждениях. Здесь клиент предварительно в офлайн подписывает соглашение о присоединении к Договору дистанционного банковского обслуживания. Бумажные документы физическое лицо получает в офисе банка. В приложении к соглашению существуют Правила размещения частными лицами средств на вкладах на 23 листах и Правила дистанционного обслуживания на 37 страницах.

В том и другом случае банки представляют вкладчикам разнообразные отчеты и выписки в электронном виде дистанционно. Если в течение 5-ти дней от владельцев счетов не поступает возражений, то считается, что совершенные операции подтверждены контрагентами.

Наши рекомендации

Как видим, клиентам кредитных учреждений непросто бывает разобраться в собственных договорных отношениях с банками. Поэтому рекомендуем все же забирать у второй стороны необходимые договоры, выписки и отчеты в бумажном виде с удостоверяющими печатями и подписями уполномоченных сотрудников. Некоторые обычно подтверждаются только распечатанным на принтере черным штампом «заверено электронно-цифровой подписью» (вполне законно), но в банковских тарифах есть пункт, предусматривающий платную услугу заверки документов синей печатью по желанию клиента.

Надо отметить, что пока судебная практика не знает прецедентов отказа финучреждений от обязательств по договору банковского вклада, заключенного через интернет-систему. Надеемся, что так оно и будет всегда. Видимо, здесь играет свою роль множество факторов: и наличие обширной нормативной базы, и надзор за банковской деятельностью её основного регулятора Банка России, который периодически избавляется от нечестных и рискованных игроков среди банков.

Боязнь отзыва лицензии и потери деловой репутации заставляет сегодня многих банкиров с оглядкой относиться к хитрым приемам ведения бизнеса. Да и государство медленно, но верно совершенствует законодательную базу, как это было совсем недавно с дополнительными комиссиями банков при кредитовании или «подстрочными» ссудными процентами, фактически превышающими те, что указаны в рекламе. Хотя согласимся с утверждением, что банковская система еще очень далека от совершенства. Средства массовой информации порой небезосновательно рассуждают о несправедливости финансового бизнеса по отношению к обществу и его гражданам.

С одной стороны, технические новинки упрощают жизнь современного человека, с другой – усложняют существование, наполняя действительность множеством компромиссов и условностей. В этом ключе советуем набраться терпения и изучать внимательно все пункты двухсторонних соглашений, даже если это займет много времени. Когда дело касается ваших личных финансов, тем более не стоит пренебрегать требованием от банка основополагающих документов с «живой» подписью уполномоченного лица и подтвержденных круглой синей печатью».

4.1.2 Общие и специальные консультации

В сети довольно много консультаций по вопросу о том, как доказать наличие вклада в банке. В основном, это консультации общего характера, но они, тем не менее, содержат полезную информацию для владельцев вкладов, заключенных онлайн.

Ниже содержаться ссылки на довольно объемные консультации общего характера, За содержание и полноту консультаций несут ответственность их авторы.

- **Ваш персональный финансист – Как проверить наличия сведений о вкладчиках АСВ в реестре?**
  https://kreditovod.com/depozity/proverit-nalichiya-svedenij-o-vkladchikah/#problema-reestrov-popravki-i-poterya-dannyh

«На сегодняшний день в Российской Федерации происходит много неурядиц в банковской сфере и несоответствий установленным нормам. Некоторые потребители банковских услуг даже не подозревают, что есть вероятность того, что придется приводить доказательства о наличии вкладов.

Банки несут обязательства перед вкладчиками, которые можно посмотреть в специальных документах. Очень часто бывает так, что пока чрезвычайная ситуация не произойдет конкретно с кем-то из близкого окружения, нас не интересуют никакие проблемы. Но на самом деле в последнее время можно наблюдать появление очень неприятных ситуаций в ведении банковской деятельности некоторых финучреждений. Именно об этом пойдет речь далее в нашей статье.

Содержание:

- Реестр вкладчиков – АСВ
- Реестры – что такое?
- Проблема реестров, поправки и потеря данных
- Сомнительные финучреждения
- Как доказать в суде, что вы являетесь держателем вклада в финучреждении?

Какие действия нужно предпринять?

Вывод

На данный момент доказать свою причастность к реестру потребителям довольно трудно даже с наличием весомых доказательств».

- **CALCULATOR24.RU – Как не стать обманутым вкладчиком. Рекомендации при размещении депозита в банке**
  http://calculator24.ru/2017/07/31/kak-ne-stat-obmanutym-vkladchikom/

- **SRAVNI.RU – Выписка банка – для чего она нужна и как её получить https://www.sravni.ru/enciklopediya/info/vypiska-banka--dlja-chego-ona-nuzhna-i-kak-ejo-poluchit/**

«Выписка из банка – это документ, отражающий движения по счёту за определённый период, а также итоговый баланс. Мы расскажем нашим читателям, для каких целей берётся выписка банка, как её заказать и какую информацию можно получить с помощью этого документа.

Содержание

1. Документ «Выписка банка»;
2. Как получить выписку из банка;
3. Электронная выписка банка;
4. Выписка банка по счету организации;
5. Особенности формирования документа;
6. Проверка банковской выписки;
7. Сомнения по поводу электронных выписок;
8. Выписка из банка: образец;
9. Какая информация указывается в выписке;
10. Как бухгалтер проверяет и обрабатывает выписки;
11. Для чего оформляется выписка из банка для физлиц».

- **ХраниДеньги – Доказательства наличия вклада: обязательна ли печать на документах http://hranidengi.ru/dokazatelstva-nalichiya-vklada-obyazatelna-li-pechat-na-dokumentah/**

Приводим некоторые из консультаций, адресованные средствами массовой информации и онлайн-юристами специально онлайн-вкладчикам:

- **Banki.ru – Как доказать наличие виртуального вклада? https://www.banki.ru/blog/artm_eyskov/7311.php**

«Короткий ответ: периодически брать выписку.

Длинный ответ.

Многие банки предлагают открыть вклад без посещения отделения, через интернет. Такие вклады могут называться по-разному: онлайн, виртуальные, дистанционные и т.п. Суть одна: клиент, уже имеющий договор на обслуживание в данном банке, может открыть новый вклад через сайт банка или (иногда) через банкомат. Ставка по такому депозиту обычно чуть выше, чем по обычному, в остальном «виртуальный» вклад не отличается от «бумажного»: по нему начисляются проценты, он застрахован в АСВ ровно на тех же условиях, деньги с него можно снять или перевести на другой счёт (на условиях, прописанных в договоре).

Однако, у «виртуальных» вкладчиков иногда возникает повод для беспокойства. В случае отзыва лицензии у банка вкладчик не имеет никаких подтверждающих наличие вклада документов. Возникает вопрос: можно ли быть уверенным, что деньги будут выплачены?

1. Давайте разберёмся, как поступать с онлайн вкладами.
   Перед «виртуальным» открытием депозита в интернете убедитесь, что вы вообще имеете дело с банком. Совет может показаться странным, но, к сожалению, невнимательность людей не имеет пределов. Неопытные интернет-пользователи перечисляют деньги анонимам, обещающим высокий процент, а потом удивляются, что «банк не платит». Организация, принимающая у вас вклад, должна быть банком с лицензией Банка России, а не неизвестным ООО, микрофинансовой организацией или просто сайтом с громким (часто «иностранным») названием.
2. Обратите внимание, что сделать онлайн вклад, не имея до этого отношений с банком, невозможно. Вы в любом случае должны хотя бы раз побывать в отделении или иным способом заключить договор с банком, предоставив «живьём» свой паспорт и прочие данные.
3. Обязательно сохраните этот договор, несмотря на то, что в нём нет конкретных данных о вашем вкладе.
4. Как и в случае с обычным вкладом, «виртуальный» депозит застрахован государством на 1,4 млн рублей (на момент публикации заметки). Соответственно, не стоит превышать эту сумму (с учётом будущих процентов). Кроме того, вы конечно помните, что все вклады одного лица в банке при расчёте суммы выплаты страховки складываются, поэтому открывать несколько виртуальных вкладов, в сумме дающих больше 1,4 млн рублей, смысла нет.
5. Для получения возмещения после отзыва лицензии у банка достаточно предъявить паспорт; по закону никакие другие бумаги не требуются, так как АСВ получает у лопнувшего банка базу данных по вкладчикам. Но в сложных случаях, когда информация о вкладах утеряна или не совсем точна, вкладчику лучше иметь на руках бумажное подтверждение своих требований к банку.
6. А потому, если банк предоставляет такую возможность, и она не слишком накладна относительно суммы вклада и процентов, закажите регулярное получение бумажной выписки (ежемесячно). Если нет, периодически заходите в банк и просите распечатать вам такую выписку. В некоторых банках её «по умолчанию» выдают без подписей и печатей, поэтому говорите, что вам нужна «заверенная выписка». Возможно, для её получения придётся написать заявление. Не обязательно делать это часто, особенно в крупном и надёжном банке, но по возможности лучше перестраховаться и иногда «освежать» выписку.
7. Если вы видите, что с банком «происходит что-то не то» (задержки с выплатой вкладов, неожиданные неприятные изменения тарифов, слухи, негативные публикации в прессе), не поленитесь и срочно сходите за выпиской.

Когда надо предъявлять выписку? Только в случае несогласия с суммой возмещения по виртуальному вкладу. В нормальной ситуации этого не требуется, но при возникновении спора с АСВ необходимо предъявить ему как можно больше доказательств, что у вас действительно был такой счёт и такая-то сумма на нём. Это прописано в документе под названием «Порядок выплаты возмещения по вкладам», п. 8.2. подпункт 3. Именно в этот момент вам пригодятся как «общий» договор на банковское обслуживание в данном банке, так и выписки по конкретному счёту/вкладу. Чем ближе дата выписки будет к дате отзыва лицензии у банка, тем лучше.

В целом, сильно беспокоиться по поводу «виртуальности» вклада не стоит, но на всякий случай лучше иметь бумажные подтверждения его существования».

- **Утро.ru – Развенчиваем мифы об онлайн вкладах http://dengi.utro.ru/articles/razvenchivaem-mify-ob-onlayn-vkladakh-1248.html**

«Ok, Google: можно ли открыть вклад онлайн?

С каждым месяцем банки все больше снижают ставки по вкладам. И на первый план теперь выходит не доходность вклада, а его комфортность. В частности, банки сами активно продвигают идею онлайн вклада, который можно открыть хоть с компьютера, хоть с мобильного телефона. Однако, если внимательно посмотреть, с этими онлайн вкладами, оказывается, не все так просто.

Онлайн вклад нельзя открыть онлайн

Да, это принципиальный момент: открыть вклад полностью в режиме онлайн сейчас нельзя. В большинстве российских банков, открывая вклад онлайн, вы не открываете его в прямом смысле слова – обычно, через свой интернет банк или мобильное приложение вы можете просто отправить заявку на открытие депозита.

Это удобно, в первую очередь, для банка, так как вы предоставляете ему свои данные (email и номер телефона) еще до того, как стали его клиентом, банк может использовать их по своему усмотрению.

Например, таким образом вы как бы даете разрешение банку звонить вам в любое время дня и напоминать о том, что вы намеревались открыть вклад. Даже если вы уже передумали, нашли более выгодный вклад в другой кредитной организации, доказать это сотрудникам колл-центра будет очень сложно – они будут звонить вам снова и снова. Если бы вы пришли в отделение открывать вклад и в последний момент передумали, такого бы не случилось.

Открыть вклад без посещения офиса сейчас можно только в кредитных учреждениях, ориентированных на интернет среду и не имеющих такое большое количество офисов, как тот же Сбербанк. Самым ярким примером в России является Тинькофф банк. В этом случае действительно все вопросы можно решить дистанционно: вы заполняете подробную анкету, отправляете ее в банк, вам перезванивает сотрудник колл-центра и вы обговариваете все условия вклада. Затем к вам приезжает сотрудник банка и вы с ним подписываете договор. Один экземпляр остается у вас, другой – у банка. После этого, чтобы вклад начал «работать», достаточно просто пополнить его с банковской карты.

Закрыть такой вклад тоже довольно просто – вы звоните в банк и сообщаете о желании закрыть вклад. После того, как вы не поддались на уговоры сотрудника оставить деньги на вкладе, в течение нескольких дней все средства, включая проценты, будут перечислены вам на карту.

Ставка по онлайн вкладам выше

Конечно, у онлайн вкладов есть приятный бонус – ставки по ним, как правило, немного выше в сравнении с обычными вкладами. Например, ставка по вкладу «Сохраняй»

в Сбербанке составляет всего 7% годовых, а по вкладу «Сохраняй Онлайн» – уже 7,40% без учета капитализации процентов.

Происходит это, опять же, за счет клиентов. Такие продукты, как правило, обходятся дешевле для банков за счет высокой удельной доли самостоятельных действий клиентов. Иными словами, за счет того, что клиент берет на себя часть обязанностей сотрудников банка, ему за это немного доплачивают. В среднем ставки могут отличаться по сравнению с аналогичными продуктами в офисе на 0,5 – 1%.

Кстати, в случае отзыва лицензии у банка вы можете не переживать за свои деньги – они будут застрахованы по тем же правилам, что и для обычных вкладов – АСВ гарантирует вернуть до 1,4 млн руб. Правда, страхование действует не во всех случаях…

Недостатки современных онлайн вкладов

К сожалению, у любого онлайн продукта есть технические недостатки. Например, мошенники могут получить доступ к вашим деньгам. Хотя банки активно продвигают саму идею онлайн банка, но за безопасностью этих самых онлайн вкладов уследить получается не всегда.

К примеру, недавно ФСБ сообщило о задержании 50 хакеров, которые украли со счетов российских банков более 1,7 млрд руб. Арест преступников, по словам представителей ФСБ, помог предотвратить хищения еще на 2,2 млрд руб. Задумайтесь, ведь среди этих миллиардов мог оказаться и ваш онлайн вклад.

Кроме того, ничего не помешает недобросовестным банкам также украсть ваши деньги. Центробанк заподозрил банки в том, что они используют кибератаки, как ширму для вывода средств со счетов. Так, по информации регулятора, с помощью ложных кибератак банки в прошлом году украли сами у себя 1,5 млрд руб. Еще полмиллиарда властям удалось перехватить до того, как деньги были выведены. Доказать, что хакеры действовали по наводке банкиров, невозможно, говорят эксперты.

Причем, банкиры крайне неохотно сообщают об атаках на их системы, так как в противном случае Банк России может заподозрить банк в нарушении стандартов безопасности.

Конечно, банкиры все отрицают и говорят, что кибератаки участились не по злому умыслу, а скорее из-захалатности. Так как программное обеспечение обновляется не часто, а обновление аппаратуры стоит дорого, банк не обновляет свои базы до тех пор, пока у него воруют по чуть-чуть. А при крупном воровстве кредитная организация и вовсе скорее всего лишится лицензии, так как будет испытывать недостаточность капитала.

И, в конце концов, нередко случаются банальные технические сбои, которые также приведут к утере денег. В последнее время во многих крупных банках наблюдались технические сбои: у россиян то списывались деньги за несовершенные операции, то наоборот, банк начислял лишнее, а затем отбирал назад.

Чаще всего такие истории благополучно разрешаются, но, согласитесь, новость о том, что с вашего вклада пропали все деньги, заставит вас понервничать.

Сама идея онлайн вклада, безусловно, хороша – за ней явно будущее. Но к этому будущему нужно как следует подготовиться. До тех пор, пока фундамент для финансовых

онлайн продуктов не будет надежным, система онлайн вкладов никогда не будет функционировать, как следует».

Из форумов:

- **https://Bankivonline.ru – КАК ПОДТВЕРДИТЬ СУЩЕСТВОВАНИЕ ОНЛАЙН ВКЛАДА ПРИ СБОЯХ?**
  https://bankivonline.ru/forum/4-548-1

Offline

Модератор

Сообщений: 494

Репутация: **0**

«Здравствуйте.

У меня ещё один вопрос по поводу вкладов «Онлайн». Открывая подобный вклад, в отличие от вклада, открытого в отделении банка, я не получаю на руки никакого документа с подписями и печатями банка, который может быть аргументом в суде в случае, «если вдруг что». Я получаю лишь номер вклада – набор цифр.

А знакомый на днях рассказал, что бывали случаи, когда подобные вклады у людей просто исчезали, то ли в результате технических сбоев, то ли в результате чего-то ещё.

Вопрос простой: если вдруг вклад «онлайн» станет недоступным, перестанет отображаться в Сбербанке онлайн и в мобильном приложении, какой есть способ доказать, что этот вклад реально есть/был? Могут ли быть подобным доказательством распечатки выписок по вкладам из кабинета пользователя, при отсутствии на них каких-либо печатей и подписей? Техника ведь всегда может давать сбои. Заранее спасибо за ответ».

SberZnaika — 2015-12-31 / 07:14 / Сообщение 2

Offline

Администратор

Сообщений: 937

Репутация: **0**

«При открытии вклада Онлайн Вы можете получить договор в письменном виде в отделении банка по месту ведения счета карты, с которой происходит списание на данный вклад. Обратиться необходимо с паспортом.

Кроме того, при совершении операций по вкладу Вы можете распечатать чек, а также обратиться в любое отделение банка с паспортом и получить справку, подтверждающую факт перечисления.»

- **YURCLUB.RU – Выписка из онлайн-сервиса банка как доказательство в суде**
  http://forum.yurclub.ru/index.php?showtopic=342901

«Здравствуйте!

Можно ли использовать выписку по лицевому счету, распечатанную из из онлайн-сервиса банка, как доказательство в суде по гражданскому делу? Нужно ли выписку полученную таким образом как-то заверять для суда? Спасибо.

Добрый день!

Да, можно предоставить выписку по лицевому счету, как доказательство. Процессуальных ограничений как сторона доказывает свою позицию достаточно мало. Другое дело, что: "Статья 67. Оценка доказательств.

1. Суд оценивает доказательства по своему внутреннему убеждению, основанному на всестороннем, полном, объективном и непосредственном исследовании имеющихся в деле доказательств.
2. Никакие доказательства не имеют для суда заранее установленной силы.
3. Суд оценивает относимость, допустимость, достоверность каждого доказательства в отдельности, а также достаточность и взаимную связь доказательств в их совокупности."

Поэтому вашу распечатку не пойми чего не пойми откуда суд может не учесть при вынесении решения. А может и учесть, без знания обстоятельств дела предугадать сложно.

Поэтому правильный алгоритм действий следующий:

1. Распечатать выписку по лицевому счету.
2. Обратиться в банк с официальным запросом (что бы банк на вашем экземпляре запроса поставил штамп о его получении) о предоставлении заверенной выписки по счету.
3. Если банк дал - предоставить в суд.
4. Если банк не предоставил выписку – ходатайствуете перед судом об истребовании доказательств, прикладывая распечатку выписки и запрос в банк.

Дальше по обстоятельствам».

- **E1.RU – Обязан ли банк заверить свою выписку?**
  https://www.e1.ru/talk/forum/read.php?f=77&i=278703&t=278703

«Регламентировано ли это чем-то, кроме «обычаев делового оборота»? ситуация (моё обращение в ЦБ):

25.03.2015 я обратился в офис банка за подтверждением зачисления на счет (вклад) средств, внесенных через банкомат на карту и перечисленных во вклад через интернетбанк. Получил выписку со счета, однако операционист наотрез отказалась заверять её подписью и печатью, мотивируя это неким указанием ЦБ.Выписка представляет собой обычный лист бумаги А4 со списком операций, отпечатанный на принтере, без каких-либо штрихкодов или других криптоотметок.

Реквизиты упомянутого «указания ЦБ» операционист распечатать и назвать отказалась.

Оставил по этому поводу в банке заявление.

Как известно, чеки, выдаваемые банкоматом, отпечатаны на термобумаге, которая быстро теряет свои свойства и через непродолжительное время документ становится нечитабельным. При использовании дистанционных технологий клиент банка остаётся без каких-либо подтверждающих документов о переводе, да ещё и без возможности их получить. Прошу разъяснить, давал ли ЦБ подобное указание, а если давал, то причины такого указания.

Считаю, что такое указание, если и было дано (а если не было, то действия сотрудников банка) нарушает права граждан на судебную защиту, так как лишает их возможности иметь и получать письменные доказательства совершённых переводов средств с использованием дистанционных технологий».

Re: Обязан ли банк заверить свою выписку?	#278710

Автор: Redline (Law) (О пользователе) Дата: 30 Мар 2015 19:48

"Положение о правилах ведения бухгалтерского учета в кредитных организациях, расположенных на территории Российской Федерации"

Выписки из лицевых счетов, распечатанные с использованием средств вычислительной техники, выдаются клиентам без штампов и подписей работников кредитной организации.

4.2. Статьи и отзывы о проблемах подтверждения операций, совершенных дистанционно

Судя по отзывам, проблема подтверждения операций, совершенных в Интернете, существует не первый год и не только для банковских вкладов.

Ниже приводится отрывок из записи блога, датированной 2013 годом.

- **Banki.ru – Опасность открытия вкладов через интернет-банк/банкомат/УДБО/СМС**
  https://www.banki.ru/blog/tsj/4368.php

«Уважаемые вкладчики, если у Вас договор вклада открыт через дистанционные сервисы, в том числе интернет-банк/банкомат/УДБО/СМС, рекомендую Вам обратиться в отделение Вашего банка и получить выписку со счета с подтверждением суммы на счете с печатью банка.

Почитал я тут в Гражданском Кодексе РФ об открытии вкладов без письменного договора. Фантастика, вот тут банкам и АСВ карта то и поперла! Уже есть случаи, когда АСВ уже отказывает в выплатам тем, кто не имеет бумажного договора вклада на руках или не может подтвердить остаток по счету выпиской из банка с печатью.

Также Привет банку на букву «А», который договора делает в одном экземпляре, для самого себя, где у вкладчика копии нет, это тот же случай. Итак, читаем закон.

Согласно подп.1. п.1. ст. 161 Гражданского Кодекса Российской Федерации сделки между банками (юридическими лицами) с гражданами должны совершаться в ПИСЬМЕННОЙ форме.

Согласно п.2. ст. 836 Гражданского Кодекса Российской Федерации Несоблюдение письменной формы договора банковского вклада влечет недействительность этого договора. Такой договор является ничтожным.
Согласно ст. 166 Гражданского Кодекса Российской Федерации ничтожная сделка недействительна независимо от признания её таковой судом.
Согласно ст. 167 Гражданского Кодекса Российской Федерации Недействительная сделка не влечет юридических последствий, за исключением тех, которые связаны с ее недействительностью, и недействительна с момента ее совершения.

То есть, если строго по закону, то без письменного договора банковского вклада банк НЕ ОБЯЗАН платить проценты по вкладу, возвращать его в срок до 2050-2100-2150 года и прочее-прочее-прочее. Банк вообще НИЧЕГО НЕ ОБЯЗАН без бумаги.

Итак, повышаем свою финансовую грамотность, читаем Гражданский Кодекс.

А еще подозрительно часто стали ломаться банковские АБС, если подумать кому это выгодно, то фактически это же выгодно и тому же АСВ, если нет бумажного договора на вклад, а база «стерлась», то выплачивать ничего не надо. И даже бумага о переводе средств из другого банка не является доказательством для суда.

И для меня очень странно, что наши российские вкладчики ища где на 0,5% ставка выше, или даже открывая дистанционные вклады через УДБО Сбербанка, не удосуживаются потратить время, заставить банк потратить 20 копеек на бумагу и получить договор и выписку со счета с печатью, откуда такая доверчивость?

Из комментариев:

@mike (@mike)

28.10.2013 18:50 #

Цитата

А вот договор по вкладу, заключенном "через интернет-банк/банкомат/УДБО/СМС" вы не получите, сама процедура такого открытия не позволит его напечатать --- нет персональной стороны-подписанта со стороны банка. (имхо)

Сугубо личный опыт. Получал договор на вклад, открытый дистанционно через систему Телебанк. Операционистка откровенно не понимала зачем, я был первым, кто обратился к ней с такой просьбой. Однако договор был напечатан, подписан и заверен печатью».

Ниже приводятся статьи, посвященные проблемам использования электронных документов в качестве доказательств.

- **Kroosp.ru – Правила подачи электронных документов в суд с 1 января 2017 года**
  http://kroosp.ru/pravila-podachi-elektronnyh-dokumentov-v-sud-s-1-yanvarya-2017-goda/

«С 1 января 2017 года процессуальные документы можно будет подавать в электронном виде не только в арбитражном, но и гражданском или административном процессе.

С 1 января 2017 года изменятся правила электронного документооборота для арбитражного, гражданского и административного процессов. Например, процессуальные документы можно будет подавать в электронном виде.

При этом соответствующие положения новой редакции АПК РФ,ГПК РФ и КАС РФ будут применяться только в судах, обладающих необходимыми техническими возможностями (ч. 4 ст. 12 Федерального закона от 23 июня 2016 г. № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти», далее – Закон № 220-ФЗ). Это значит, что если, к примеру, в суде общей юрисдикции нет возможности получать документы в электронном виде или извещать участников процесса через интернет, суд будет работать по прежним правилам.

Подача электронного документа для суда

Все процессуальные документы (иски, заявления, жалобы, ходатайства и т. д.) теперь можно будет подавать в суды как в бумажном, так и в электронном виде (ч. 7 ст. 4 АПК РФ, ч. 1.1 ст. 3 ГПК РФ, ч. 2 ст. 45 КАС РФ).

В арбитражном процессе электронный документооборот действует уже сейчас. Однако заявление об обеспечении иска, исковое заявление с ходатайством об обеспечении иска, заявление об обеспечении имущественных интересов и ходатайство о приостановлении исполнения судебных актов можно было подавать только в бумажном виде. С 1 января 2017 года заявитель вправе подать такие документы в электронной форме, но они должны быть подписаны усиленной квалифицированной электронной подписью (ч. 1 ст. 92, ч. 1 ст. 99, ч. 1 ст. 125, ч. 1 ст. 265.1, ч. 1 ст. 283, ч. 3 ст. 291.6, ч. 3 ст. 308.4 АПК РФ).

Также с 1 января 2017 года правила электронного документооборота начнут действовать в гражданском и в административном процессах, а не только арбитражном. Любой процессуальный документ можно будет подать в суд общей юрисдикции в электронном виде. Для этого нужно будет заполнить специальную форму на сайте суда.

По общему правилу документы, которые подаются в суд общей юрисдикции в электронном виде, не нужно будет скреплять усиленной квалифицированной электронной подписью.

Однако так же, как и в арбитражном процессе, появятся документы, которые можно подать в суд общей юрисдикции в электронной форме, только если они будут скреплены усиленной квалифицированной электронной подписью. К ним относятся:

- заявление об обеспечении иска (ч. 1 ст. 139 ГПК РФ);
- заявление о применении мер предварительной защиты по административному иску (ч. 1.1 ст. 86 КАС РФ);
- исковое заявление, которое содержит ходатайство об обеспечении иска (ч. 4 ст. 131 ГПК РФ);

- административное исковое заявление, которое содержит ходатайство о применении мер предварительной защиты (ч. 9 ст. 125 КАС РФ);
- ходатайство о приостановлении исполнения судебных постановлений (ч. 1 ст. 381, ч. 1 ст. 391.5 ГПК РФ).

Требования к техническим и программным средствам при использовании усиленной квалифицированной электронной подписи устанавливает Верховный суд РФ и Судебный департамент при Верховном суде РФ (ст. 4 Закона № 220-ФЗ) в рамках своих полномочий.

Подача электронного документа в качестве доказательства

Суды будут принимать в качестве письменных доказательств электронные документы. Если копии документов представлены в электронном виде, суд может потребовать представить подлинники таких документов (абз. 1 ч. 3 ст. 75 АПК РФ, ч. 1 ст. 71 ГПК РФ, ч. 1.1 ст. 70 КАС РФ). В КАС РФ первоначально электронные документы были названы в качестве отдельного вида доказательств. Теперь электронные документы отнесли к письменным доказательствам.

Чтобы суд принял электронный документ в качестве доказательства, нужно подтвердить достоверность электронного документа. Например, если данные электронного документа повторяются в бумажной переписке, это подтверждает его содержание. Электронную версию документа можно заверить у нотариуса. Нужно помнить, что нотариус удостоверяет только то, что видит на экране, и подтвердит личности отправителя и получателя. Нотариально можно подтвердить не только содержания документа, но и контактные данные стороны, если они видны на экране. Также электронный документ можно проверить с помощью компьютерно-технической экспертизы и т. д.

Лица, участвующие в деле, смогут получать копии судебных актов и постановлений в виде электронных документов (ч. 1 ст. 41 АПК РФ; ч. 1 ст. 35 ГПК РФ; ч. 4 ст. 45 КАС РФ). Речь идет о тех актах, которые суд принимает в виде отдельных документов. Протокольных определений такое правило не касается: их суды не будут составлять ни на бумаге, ни в электронной форме.

Для этого суды будут составлять судебные акты и постановления в двух формах: бумажной и электронной (ч. 5 ст. 15 АПК РФ; ч. 1 ст. 13 ГПК РФ; ч. 1.1 ст. 16 КАС РФ). Судебный акт, который составлен в электронной форме, судья должен будет заверить усиленной квалифицированной электронной подписью. В дополнение к электронной форме судье нужно составить судебный акт на бумажном носителе. Это правило распространяется как на все решение в целом, так и на резолютивную часть, которую выносит суд, когда откладывает составление мотивированного текста на срок не более пяти дней (ч. 3 ст. 176 АПК РФ; ч. 1 ст. 199 ГПК РФ; ч. 3 ст. 177 КАС РФ).

По общему правилу арбитражный суд не будет высылать участникам процесса бумажный вариант судебного акта, который он изготовил в форме электронного документа. Этот судебный акт будет размещаться на официальном сайте арбитражного суда в Интернете в режиме ограниченного доступа (в арбитражном процессе – не позднее следующего дня после дня, когда суд его принял). Но по ходатайству участвующих в деле лиц суд в течение пяти дней вышлет им копию судебного акта на бумажном носителе заказным письмом или вручит им под расписку.

Если в суде не будет возможности составить акт в форме электронного документа, действуют прежние правила: составляется только бумажный вариант. Такой акт по общим правилам направляется участвующим в деле лицам по почте или вручается под расписку.

Такие правила содержатся в части 1 статьи 177 и в части 1 статьи 186 Арбитражного процессуального кодекса РФ.

Кроме того, судья не будет составлять судебный акт в электронной форме в тех случаях, когда он содержит сведения, которые относятся к государственной или иной охраняемой законом тайне, и суд рассматривал дело в закрытом судебном заседании (ч. 5 ст. 15 АПК РФ)».

В следующих статьях рассматриваются понятие вопросы юридической природы и статуса электронного документа, проблемы отсутствия в российском законодательстве критериев достоверности данных, содержащихся в электронном документе:

- **СЕДЕЛЬНИКОВА Д.В. Проблемы применения электронного доказательства в гражданском и арбитражном процессах https://cyberleninka.ru/article/n/problemy-primeneniya-elektronnogo-dokazatelstva-v-grazhdanskom-i-arbitrazhnom-protsessah;**
- **ЗАХАРЕНКО В.В. Проблема представления электронного документа в качестве доказательства в гражданском и арбитражном процессах https://cyberleninka.ru/article/n/problema-predstavleniya-elektronnogo-dokumenta-v-kachestve-dokazatelstva-v-grazhdanskom-i-arbitrazhnom-protsessah;**
- **Электронные доказательства в суде https://blog.casebook.ru/elektronnye-dokazatelstva-v-sude/.**

«Электронные доказательства в суде

Интернет, смартфоны, электронные приложения, видео-регистраторы и другие всевозможные гаджеты окружают нас ежедневно и повсюду. Но вопрос принятия подобных электронных доказательств решается в каждом случае индивидуально по усмотрению суда. Раньше суды приходили к мнению, что данные электронной почты, скриншоты или ролики на youtube не являются надлежащими доказательствами. Но судебная практика меняется с учетом последних технологических тенденций.

Проблемы и перспективы развития электронных доказательств

Существует ряд проблем, связанных с применением электронных документов и электронных доказательств.

Отсутствие определения электронных доказательств
В соответствии с п. 11.1 ст. 2 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» электронный документ – это документированная информация, представленная в электронной форме, т.е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах. Электронный документ следует отличать от электронного сообщения. Согласно указанному Закону электронное сообщение

– это информация, переданная или полученная пользователем информационно-телекоммуникационной сети (п. 10 ст. 2).

Однако данное определение не в полной мере охватывает все электронные доказательства, например, электронные программы, компьютерные программы, СМС-оповещения, скриншоты.

Отсутствие возможности получения доказательств в процессуальном порядке В ряде случаев электронные документы не принимаются, поскольку получены не в процессуальном порядке. Суд не может считать доказанными обстоятельства, подтверждаемые только копией документа или иного письменного доказательства, если утрачен и не передан суду оригинал документа, и представленные каждой из спорящих сторон копии этого документа не тождественны между собой, и невозможно установить подлинное содержание оригинала документа с помощью других доказательств. А электронный документ не считается оригиналом документа.

АПК РФ содержит дополнительное требование к допустимости электронных доказательств: наличие специального санкционирующего их использование положения либо в нормах законодательства, либо в договоре, заключенном между сторонами. А в законодательстве не всегда содержится соответствующая ссылка на допустимость подобных доказательств.

Особенности подписания электронных документов

Внесенными в Кодекс административного судопроизводства РФ, устанавливается, что административное исковое заявление, заявление, жалоба, представление и иные документы могут быть поданы в суд в электронном виде посредством заполнения формы, размещенной на официальном сайте соответствующего суда в информационно-телекоммуникационной сети «Интернет». При этом определено, что документы, полученные посредством факсимильной, электронной или иной связи, а также документы, подписанные электронной подписью, могут быть допущены в качестве письменных доказательств. Если копии документов представлены в суд в электронном виде, суд может потребовать представления подлинников этих документов. А это означает, что документы должны иметь электронную подпись и не всегда являются достаточными письменными доказательствами.

Вместе с тем, перспективы развития электронных доказательств в суде можно увидеть уже сейчас:

1. Развитие поправок в электронное судопроизводство. Еще лет 20 назад нельзя было представить и подачу исков в суд и сбор доказательств в электронном виде, однако сегодня мы активно пользуемся и системой «Мой Арбитр», и специальными сервисами Casebook, Caselook, а также имеем возможность подачи иска в электронном виде.
2. Наличие законодательных основ применения электронных доказательств. И в АПК РФ, и в ГПК РФ и в КАС РФ существуют ссылки на возможность использования именно электронных доказательств как средств доказывания юридических фактов. А это означает, что на законодательном уровне данные доказательства признаны допустимыми.

3. Принятие судами электронных доказательств.
   В настоящее время многие суды уже используют электронные доказательства, поскольку они позволяют установить юридически значимые факты при отсутствии прямых доказательств, документов на бумажных носителях.

Переписка по электронной почте

Наиболее часто в настоящее время работник и работодатель, а также контрагенты общаются посредством электронной переписки. Однако электронная переписка применяется только в определенных случаях. Так, согласно п. 3 ст. 75 АПК РФ, документы, полученные посредством факсимильной, электронной или иной связи, в том числе с использованием информационно-телекоммуникационной сети Интернет, допускаются в качестве письменных доказательств в случаях и в порядке, которые установлены АПК РФ, другими федеральными законами, иными нормативными правовыми актами или договором.

Если в договоре установлено подтверждение факта осуществления работ, услуг, по электронной почте, то суд примет это в качестве доказательств. Например, в Постановлении Девятого арбитражного апелляционного суда от 16.02.2015 N 09АП-59251/2014-ГК по делу NA40-128123/14 суде было подтверждено, что с почтового электронного ящика были направлены 13 писем, содержащих приложения в виде актов о приемке выполненных работ, счета-фактуры и ежемесячные отчеты о продвижении сайта. Содержания направленных писем полностью идентично письмам, приложенных Ответчиком. Суд установил, что факт оказания услуг Ответчиком, их принятие Истцом дополнительно подтверждается деловой перепиской по электронной почте, имевшей место между Сторонами в течение всего срока исполнения Договора, копии писем представлены в материалы дела.

Скриншот страницы Интернет-ресурса

Скриншоты Интернет-страниц также могут служить в качестве доказательств в суде. При этом в отличие от электронной переписки для признания скриншота станицы в Интернете не нужно соответствующего указания в договоре. В частности, скриншоты страниц часто используются для привлечения к административной ответственности.

В качестве примера можно назвать решение Арбитражного суда Забайкальского края от 30.03.2017 по делу № A78-1667/2017. В данном судебной споре был рассмотрен случай, когда оператор связи был привлечен к ответственности, поскольку оператор связи не ограничивает доступ к запрещенному информационному ресурсу. И в качестве доказательств правомерного привлечения к административной ответственности суд принял скриншот электронной страницы.

Согласно части 1 статьи 26.2 КоАП Российской Федерации доказательствами по делу об административном правонарушении являются любые фактические данные, на основании которых судья, орган, должностное лицо, в производстве которых находится дело, устанавливают наличие или отсутствие события административного правонарушения, виновность лица, привлекаемого к административной ответственности, а также иные обстоятельства, имеющие значение для правильного разрешения дела. Таким образом, скриншоты подтверждают наличие события административного правонарушения.

Скриншоты также рассматриваются судами при рассмотрении споров между контрагентами. Так, в решении Арбитражного суда апелляционной инстанции г. Владивосток от 30 марта 2017 года по делу по делу № А51-26305/2015. Именно с помощью скриншота было доказан факт наличия переписки между компаниями, а также согласование передачи доверенности на водителя для произведения в адрес Покупателя отгрузки товара. Это подтверждает возможность использования скриншота в отношении взаимоотношений между контрагентами.

Данные видеорегистратора

Данные видеорегистратора нигде не поименованы в качестве допустимых доказательств. Вместе с тем, если говорить о доказательственной базе в отношении нарушения правил дорожного движения, то такое доказательство используется достаточно давно. И это связано с наличием соответствующей нормы в Кодексе об административных правонарушениях. На основании части 3 статьи 28.6 КоАП РФ в случае выявления административного правонарушения, предусмотренного главой 12 настоящего Кодекса и зафиксированного с применением работающих в автоматическом режиме специальных технических средств, имеющих функции фото- и киносъемки, видеозаписи, или средств фото- и киносъемки, видеозаписи, протокол об административном правонарушении не составляется, а постановление по делу об административном правонарушении выносится без участия лица, в отношении которого возбуждено дело об административном правонарушении.

В решении Пермского краевого суда от 21.10.2013 по делу N 7-1031-2013/21-605-2013 суд признал правильным привлечение к административной ответственности автовладельца. Доказательственной базой нарушения являются две фотографии транспортного средства и зафиксированное время, в течение которого автомобиль был припаркован в запрещенном месте.

В решении Промышленного районного суда г.Смоленска от 25.03.2017 по делу № 5-275/2017 суд пришел к выводу о том, что машина стала участником ДТП, виновный уехал. Сосед передал запись ДТП с видеорегистратора. Суд, приняв во внимание данные доказательства, а также отсутствие обстоятельств, отягчающих административную ответственность, личность виновного, его материальное положение, признание вины и находит необходимым определил в качестве меры наказания административный штраф в размере 1000 руб.

СМС-доказательства

СМС-сообщения, а также сообщения, направляемые с помощью специальных программ для мобильных телефонов, уже достаточно давно вошли в нашу жизнь. Но СМС-сообщения также являются доказательствами в суде.

В качестве примера можно назвать Апелляционное определение Свердловского областного суда от 20.05.2016 по делу N 33-8564/2016. В данном судебном споре рассматривался вопрос об установлении факта трудовых отношений. Работник в качестве доказательств наличия трудовых отношений представил СМС-сообщения и электронную переписку.

К существенным признакам трудовых правоотношений, позволяющим отграничить их от других видов правоотношений, относятся: личный характер прав и обязанностей работника, обязанность работника выполнять определенную, заранее обусловленную трудовую функцию, выполнение трудовой функции в условиях общего труда с подчинением правилам внутреннего трудового распорядка, возмездный характер трудового отношения. Трудовые отношения между работником и работодателем могут возникать на основании фактического допущения работника к работе с ведома или по поручению работодателя или его уполномоченного на это представителя в случае, когда трудовой договор не был надлежащим образом оформлен (ч. 3 ст. 16 Трудового кодекса РФ). Соответственно, СМСки стали доказательством того, что работник приступил к работе.

Однако существует и противоположная практика. В Апелляционном определении Санкт-Петербургского городского суда от 05.10.2016 N 33-19528/2016 по делу N 2-6626/2015 суд указал, что представленные истцом в качестве доказательств распечатки СМС-сообщений не отвечают требованиям допустимости доказательств, установленным п. 7 ст. 67 ГПК РФ.

Использование программы Skype

Скайп дает возможность обмениваться информацией, файлами, фотографиями, текстовыми сообщениями. Соответственно, подобная переписка также может являться доказательством в суде. Статьей 434 Гражданского кодекса Российской Федерации предусмотрено, что договор в письменной форме может быть заключен путем составления одного документа, подписанного сторонами, а также путем обмена письмами, телеграммами, телексами, телефаксами и иными документами, в том числе электронными документами, передаваемыми по каналам связи, позволяющими достоверно установить, что документ исходит от стороны по договору.

В Постановлении Арбитражного суда Московского округа от 01.02.2017 N Ф05-21794/2016 по делу N А40-56723/16 суд рассматривал факт обмена документами посредством использования скайпа. Ответчик в материалы дела представил копию документа, поименованного договором займа, подписанного от имени генерального директора компании, и пояснил, что данный договор был получен им в электронном виде с использованием системы «Skype» от истца. Суд установил, что подлинник договора займа не представлен и сам истец факт подписания данного договора отрицает.

Использование WhatsApp

Еще одним мессанджером, используемым компаниями и физическими лицами, является вотсап. В Решении Арбитражного суда Республики Карелия от 19.09.2016 по делу N А26-4401/2016 общество признано виновным в совершении административного правонарушения, предусмотренного частью 4 статьи 15.25 КоАП РФ. Действия его квалифицированы как невыполнение резидентом в установленный срок обязанности по получению на свои банковские счета в уполномоченном банке иностранной валюты, причитающейся за переданный нерезиденту товар. Общество привлечено к административной ответственности в виде штрафа на сумму 39 717,96 руб.

Вместе с тем, принимая во внимание фактические обстоятельства дела, степень общественной опасности совершенного правонарушения и характер данного деяния, а именно: полное погашение задолженности по поступлению валютной выручки в рамках

спорного договора контракта до проведения проверки и обнаружения правонарушения, отсутствие доказательств пренебрежительного отношения общества к формальным требованиям публичного права, переписка с контрагентом по мессенджеру (скайпу, вотсапу), суд считает необходимым применить положения, изложенные в пункте 2 Постановления Конституционного суда Российской Федерации от 25.02.2014 N 4-П и снизить административную санкцию ниже низшего предела, назначенного в рамках спорного постановлением в пределах санкции, предусмотренной частью 4 статьи 15.25 КоАП РФ.

Таким образом, скайп и вотсап в совокупности с другими доказательствами признаются в качестве допустимых.

Применение электронных доказательств все больше находит отражение в судебной практике. Однако, для повсеместного применения электронных доказательств требуется внесение соответствующих поправок в нормативно-правовые акты».

- **Фемида.Science – Электронные доказательства в гражданском судопроизводстве**
  http://femida-science.ru/index.php/item/213-elektronnye-dokazatelstva-v-grazhdanskom-sudoproizvodstve

«Юрловская А.А.
ФГБОУВО «Российский государственный университет правосудия»
студентка 3 курса

Одним из самых распространенных видов доказательств в гражданском процессе являются письменные доказательства.

С 1 января 2017 г. вступили в силу изменения в ст. 71 ГПК РФ, в соответствии с которыми в числе письменных доказательств выделяется такое доказательство, как документы, подписанные электронной подписью. Однако кроме электронных документов с электронной подписью существуют электронные письма и сообщения, не содержащие электронной подписи, которые чаще всего и используются в электронной переписке.

Таким образом, все документы, полученные посредством электронной связи и представляемые в судопроизводстве, делят на две группы: электронные документы и электронные сообщения.

Рассмотрим первую группу электронных доказательств. «Электронный документ – документированная информация, представленная в электронной форме, т. е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах». Нельзя не согласиться с А. Вершининым в том, что электронный документ не отличается от информации, которая может составлять содержание «бумажных» документов.

Перечень доказательств ч.1 ст. 55 ГПК является исчерпывающим, в нём не содержится упоминание об электронных документах. Однако ст. 71 ГПК предусматривает возможность их использования. Документ в гражданском процессе рассматривается «как разновидность письменных доказательств». Однако электронный документ имеет ряд признаков, отличающих его письменных документов.

Информации, которая может составлять содержание электронного документа, не отличается от той, которая может составлять содержание иных видов документов. Его форма является его главным отличительным признаком по сравнению с другими видами документов.

Для определения достоверности содержащейся в электронном цифровом документе информации важное значение имеет наличие в нем определенных реквизитов. Одним из них является подпись. Она позволяет провести проверку подлинности электронного документа и идентифицировать подписавшее лицо.

«Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию».

Электронная подпись обладает и рядом проблем: 1) «пакетный» характер, 2) платность. Под «пакетностью» стоит понимать то, что определенный вид электронной подписи содержит в себе доступ лишь к ограниченному набору площадок, сервисов (портал госуслуги, роспатент), в связи с этим она может иметь ограниченный функционал. Для того, чтобы избавиться от данных ограничений, лицу требуется оплатить каждый дополнительный сервис.

С 1 января 2017 г. в российском гражданском процессе появилась возможность подавать документы в электронном виде (ч.1.1 ст. 3 ГПК РФ), но с использованием усиленной квалифицированной электронной подписи. Для этого нужно заполнить специальную форму на сайте суда.

В Приказе Судебного департамента N 251 для усиленной квалифицированной цифровой подписи установлен особый формат – PKCS#7. Для ее использования нужен ключ, который является уникальной последовательностью символов. В качестве ключа простой электронной подписи используется учетная запись физического лица в ЕСИА.

Заявление об обеспечении иска, исковое заявление, содержащее ходатайство об обеспечении иска, должно быть подписано усиленной квалифицированной электронной подписью.

Большинство оснований для отклонения электронного документа связано непосредственно с электронной подписью: не подписано усиленной квалифицированной электронной подписью; электронная подпись не соответствует виду или формату, установленным порядком подачи документов; усиленная квалифицированная электронная подпись не прошла проверку: истек срок действия сертификата электронной подписи на момент подписания документа.

Таким образом, электронная подпись является важнейшим элементом для подачи документа в электронном виде.

Для того, чтобы электронные документы были признаны допустимыми доказательствами по делу, они должны соответствовать определенным условиям. М.В. Горелов обосновывает выделение следующих условий допустимости электронных доказательств.

1. Требованием допуска электронного документа в гражданском процессе в качестве доказательства является «доступность в понимании».

2. Условием допуска следует рассматривать возможность идентификации его автора, которая может осуществляться с помощью электронно-цифровой подписи, возможность которой осуществима только в случае, когда установлена подлинность электронно-цифровой подписи.
3. Основанием для допуска является соблюдение условий, гарантирующих целостность документа, которые зависят от особенности создания, хранения, передачи по каналам связи электронного документа.
4. Современный источник информации должен обладать таким дополнительным свойством, как контролепригодность – возможность проведения контроля достоверности электронного документа.

Обратимся ко второй группе электронных доказательств. С помощью электронной переписки стороны доказывают направление юридически значимых сообщений (уведомлений, претензий, актов, отчетов и др.), а также конкретные обстоятельства дела. Несмотря на то, что зачастую электронная переписка является ключевым доказательством по делу, суды хоть и принимают ее в качестве доказательства, но не всегда на нее ссылаются в мотивировочной части судебных актов.

Более того, следует отметить, что переписка, которая ведется посредством электронной почты, не принимается в качестве доказательства по делу в случае, если не была предусмотрена договором, в договоре нет указания на электронные адреса сторон, а другая сторона оспаривает существование такой переписки.

Определение понятия «электронное письмо» федеральное законодательство не содержит, однако содержит определение понятия «электронное сообщение» (это информация, переданная или полученная пользователем информационно-телекоммуникационной сети). Электронное сообщение имеет статус документа, если оно заверено электронно-цифровой подписью.

Для использования электронных материалов в качестве письменного доказательства в суде необходимо обеспечить порядок установления их достоверности. В случае с электронными документами все предельно ясно: законодатель указывает на обязательное наличие в них электронной подписи.

Однако если речь идет об электронной переписке, то у суда могут появиться сомнения относительно ее достоверности в качестве доказательства, так как она не всегда заверяется электронной подписью. Возникают вопросы относительно установления личности их отправителя.

Для того, чтобы использовать электронную переписку в качестве доказательства в суде, ей нужно придать юридическую силу. Обмен электронными письмами нужно предусмотреть в договоре. Суды признают электронную переписку в качестве доказательства, если можно достоверно установить, от кого исходило сообщение и кому оно адресовано. При этом суды презюмируют, что отправка сообщения с указанного в договоре адреса электронной почты свидетельствует о совершении действий самим лицом, пока не доказано обратное.

Отправленное электронное письмо либо сообщение сохраняется в памяти компьютера, с которого оно было отправлено, либо на сервере почтовой службы (возможно подтверждение их отсылки с конкретного компьютера или IP-адреса). Однако встает

вопрос о возможности допуска третьего лица к определенному компьютеру для отправки с него того или иного письма, сообщения. Кроме этого, нужно конкретное указание в договоре на тот факт, что переписка должна вестись только с тех электронных адресов, которые указаны в реквизитах сторон.

Прежде чем представить электронную переписку в качестве доказательства в тот или иной суд, ей нужно придать юридическую силу. Существует несколько способов: обеспечение электронной корреспонденции у нотариуса, подтверждение их подлинности судебной экспертизой.

ГПК РФ и ч. 2 ст. 102 Основ законодательства РФ о нотариате не допускают возможности обеспечения нотариусом доказательств по делам, находящимся в производстве суда. Однако в силу ч. 1 ст. 102 Основ законодательства РФ о нотариате до возбуждения гражданского дела в суде нотариусом могут быть обеспечены необходимые для дела доказательства, если имеются основания полагать, что представление доказательств впоследствии станет невозможным или затруднительным.

Протокол осмотра Интернет-ресурса подписывается участвующими в осмотре лицами, нотариусом и скрепляется печатью нотариуса. Пленум Верховного Суда РФ в своем Постановлении подтвердил действенность нотариальной процедуры обеспечения доказательств, а судебная практика доказала эффективность данного института защиты прав.

Юридическая сила электронной переписке может быть придана и в ходе проведения судебно-технической экспертизы. Заключение эксперта используется для подтверждения обстоятельств дела. Ее проведение возможно в любой стадии процесса до вынесения судом решения.

Использование электронных доказательств в гражданском процессе является перспективным направлением развития института доказательств и доказывания. Рассмотрим это на конкретных примерах.

В одном деле банк объявил выговор директору службы безопасности за то, что тот одобрил заемщику кредит, не проверив необходимые сведения о нем. Проверять эти сведения сотрудник был обязан на основании инструкции по обеспечению экономической безопасности бизнеса. Работник обжаловал приказ о наложении дисциплинарного взыскания. В суде он настаивал на том, что не был ознакомлен под роспись с указанной выше инструкцией. Суд установил, что инструкция высылалась ему по электронной почте с целью ознакомления личного состава подразделения банка, и в силу своей должности он был обязан и сам ознакомиться с ее содержанием (это подтверждала выписка из архива электронной переписки). Причем работник был ознакомлен с порядком использования корпоративной электронной почты под роспись. Кроме того, аналогичные обязанности по идентификации заемщиков были предусмотрены в должностной инструкции, с которой работник тоже был ознакомлен под роспись. На этом основании суд отказал работнику в иске.

Во втором случае ситуация немного иная. Кадровые документы, полученные от работника (направленные работнику) в мобильном приложении, не являются доказательством, если ТК РФ для таких документов устанавливает письменную форму.

В пользу традиционной письменной формы общения с работником свидетельствует и решение Стрежевского городского суда. В названном деле работник направил заявление об увольнении посредством WhatsApp, а работодатель, недолго думая, издал приказ об увольнении по п. 3 ч. 1 ст. 77 ТК РФ. Впоследствии работник обратился в суд с требованием о восстановлении на работе. Суд в решении отметил, что копия приказа об увольнении, полученная посредством электронной коммуникации через приложение WhatsApp, не может служить доказательством обращения работника к работодателю с заявлением об увольнении по собственному желанию, не может быть доказательством добровольного волеизъявления на увольнение по п. 3 ч. 1 ст. 77 ТК РФ.

Таким образом, предоставление сторонам возможности ссылаться на электронную переписку в процессе доказывания своей позиции, если она позволяет установить получателя, отправителя и содержание письма, а также получена законными способами, не противоречит основам гражданского процессуального законодательства.

Для широкого использования электронных доказательств в гражданском судопроизводстве необходимо принять некоторые меры.

1. Внести некоторые изменения в ГПК РФ: включить понятие электронного документа как доказательства, закрепить правовые гарантии его использования, гарантии достоверности, определенный процессуальный порядок исследования соответствующих источников в судебном заседании.
2. Обеспечить возможность аутентификации и идентификации.
3. Разработать правовые требования относительно формы электронных доказательств.

Широкое использование электронных доказательств в ГПК РФ позволяет решить также проблему развития электронного документооборота в России, технического оснащения судебных органов, доступности судебной защиты».

4.3. Документы, материалы, комментарии о направлениях развития законодательства

4.3.1. Законодательство и материалы о совершении сделок с использованием электронной платформы

С актуальным текстом законопроекта "О совершении сделок с использованием электронной платформы", а также с иными документами - пояснительной запиской к законопроекту, где содержится анализ возникающих проблем, а также отзывами Правительства на внесенные законодательные предложения можно ознакомиться на официальном сайте Государственной Думы по адресу: http://sozd.duma.gov.ru/bill/617867-7.

Состав представленных на странице документов в процессе обсуждения законопроекта постоянно пополняется. Все документы расположены в хронологическом порядке.

Ниже представлен обзор документа – http://www.consultant.ru/law/hotdocs/56335.html/.

«Депутаты предлагают законодательное регулирование отношений по заключению сделок с финансовыми организациями с использованием электронной платформы

Проект Федерального закона N 617867-7 "О совершении сделок с использованием электронной платформы"

Согласно законопроекту, электронная платформа представляет собой информационную систему, обеспечивающую удаленное взаимодействие финансовых организаций с потребителями финансовых услуг в целях совершения сделок, направленных на предоставление банковских, страховых услуг, услуг на рынке ценных бумаг, а также иных услуг финансового характера.

Правила электронной платформы являются договором присоединения и определяют права и обязанности участников электронной платформы и оператора электронной платформы при совершении сделок с ее использованием.

В правилах электронной платформы должны содержаться в числе прочего:

- требования к участникам электронной платформы;
- виды сделок, совершаемых с использованием электронной платформы;
- порядок допуска участников электронной платформы к программно-техническим средствам электронной платформы;
- порядок совершения сделок с использованием электронной платформы, включая порядок обмена электронными документами между участниками электронной платформы;
- порядок и объем размещения оператором электронной платформы в информационно-коммуникационной сети "Интернет" информации о предложениях финансовых организаций о совершении сделок с использованием электронной платформы;
- порядок и сроки информирования оператором электронной платформы потребителя финансовых услуг о списании денежных средств со специального счета (зачислении денежных средств на специальный счет);
- порядок и сроки направления распоряжений оператора электронной платформы о списании денежных средств со специального счета по указанию потребителя финансовых услуг. При этом такой срок не может превышать трех рабочих дней;
- ответственность оператора электронной платформы перед участниками электронной платформы;
- порядок ведения учета денежных средств, принадлежащих каждому потребителю финансовых услуг, при учете на специальном счете денежных средств нескольких потребителей финансовых услуг, если такой учет осуществляется оператором электронной платформы;
- требования к банку, привлекаемому оператором электронной платформы для проведения идентификации потребителей финансовых услуг при их личном присутствии, а также их представителей, выгодоприобретателей, бенефициарных владельцев, порядок такого привлечения;
- порядок подачи через электронную платформу потребителями финансовых услуг заявлений о несогласии с размером возмещения по договорам банковского счета (вклада) и дополнительных документов в государственную корпорацию «Агентство по страхованию вкладов», обосновывающих требования потребителя финансовых услуг.

Предусматривается, что нормативным актом Банка России могут быть установлены также дополнительные требования.

Оператор электронной платформы не вправе совмещать свою деятельность с деятельностью кредитной организации, некредитной финансовой организации, за исключением деятельности организатора торговли, депозитария, специализированного депозитария или регистратора.

Минимальный размер собственных средств оператора электронной платформы должен составлять 100 миллионов рублей.

Оператор электронной платформы предоставляет сторонам сделки возможность осуществить расчеты по заключенным с использованием платформы сделкам с использованием специального счета оператора такой платформы либо сервиса быстрых платежей платежной системы Банка России.

Расчеты по сделкам, совершаемым с использованием электронной платформы, осуществляются с использованием специального счета или, если предусмотрено правилами электронной платформы, - с использованием сервиса быстрых платежей.

Денежные средства потребителей финансовых услуг не могут зачисляться на счета оператора электронной платформы, на которых находятся его собственные денежные средства.

Специальный счет может быть открыт оператору электронной платформы в кредитной организации, являющейся оператором национально значимой платежной системы, либо в кредитной организации, которой присвоен кредитный рейтинг не ниже уровня, установленного Советом директоров Банка России.

Законопроектом предусмотрено создание единого реестра финансовых транзакций, в котором будет аккумулироваться информация об обязательствах финансовой организации перед потребителем финансовых услуг по договорам банковского счета (вклада), заключенным с использованием электронной платформы.

Информация о сделках, заключаемых с использованием электронной платформы, доступ к которой предоставляется регистратором финансовых транзакций, считается достоверной, пока в судебном порядке не доказано иное».

4.3.2. Реализация проекта «Маркетплейс» http://www.cbr.ru/finmarket/market_place/

Проект «Маркетплейс» запущен Банком России совместно с участниками рынка в декабре 2017 года. Цель проекта – организация системы дистанционной розничной дистрибуции финансовых продуктов (услуг) и регистрации финансовых сделок. Информация о заключенных сделках и позициях по ним будет вестись на платформе регистратора финансовых сделок, которая представляет собой систему хранения и сбора данных о заключенных сделках и позициях по ним. Планируется, что по запросу клиенту будут предоставляться выписки из реестра для использования в качестве юридически значимой информации (например, в судах).

По указанной выше ссылке расположены презентация проекта, а также ответы на некоторые вопросы.

4.3.3. Комментарии и мнения экспертов, материалы СМИ

- **Banki.ru – «Маркетплейс»: как это работает**
  https://www.banki.ru/news/columnists/?id=10519643

«Подробно о тестировании маркетплейса ЦБ и дальнейших этапах его развития Роман Халанский, а также Елена Чайковская (советник первого заместителя председателя Банка России) и банки, участвующие в рабочей группе маркетплейса («Ак Барс», «Зенит», Совкомбанк), расскажут 27 июня на форуме FinWin 2018.

Итак, давайте по порядку. Проект «Маркетплейс» позволит всем гражданам России пользоваться банковскими продуктами дистанционно: открывать вклады, получать кредиты, покупать ценные бумаги, страховые продукты, например ОСАГО или каско. Проще говоря, проект «Маркетплейс» позволит жителям Хабаровска открывать вклады в московских банках, и наоборот, а люди, проживающие в отдаленных уголках страны, смогут взять кредит не только в одном-двух госбанках, представленных в радиусе 200 километров.

Очевидно, что сейчас потребители финансовых услуг в нашей стране такой возможности лишены. Нужна идентификация человека в офисе банка или любого другого финансового института, удаленная идентификация должна заработать с 1 июля, когда будет дан старт Единой биометрической системе (в систему можно будет направлять изображения лиц и слепки голосов. Вместе с информацией, хранящейся на сайте госуслуг, эти сведения и позволят получать финансовые услуги дистанционно).

Банки.ру уже много лет работает как финансовый супермаркет, на сегодняшний день у нас на сайте клиенты оставляют более 100 тыс. заявок на различные финансовые продукты. Сервис, который позволит открывать вклады прямо на сайте Банки.ру, будет с радостью воспринят нашими клиентами. В настоящее время доезжают до банка порядка 75–80% клиентов, оставивших заявку на вклад на сайте Банки.ру, а мы хотим, чтобы с помощью сервиса «Маркетплейс» доля таких клиентов возросла до 100%.

Теперь об архитектуре проекта.

За короткое время – всего за два месяца – были интегрированы совершенно разные участники системы: Банки.ру, Московская биржа, НРД и банки-партнеры (Совкомбанк, «Ак Барс», «Центр-инвест», банк «Зенит»).

Узнайте, как будет происходить процесс интеграции финансовых компаний в маркетплейс ЦБ и чего ждать участникам рынка, из первых уст – от представителей ЦБ, Банки.ру, банка «Ак Барс», банка «Зенит» и Совкомбанка –27 июня на форуме FinWin 2018.

Все взаимодействие с клиентом-физлицом ведет Банки.ру. То есть мы занимаемся привлечением клиентов, отображением у себя на сайте информации о финансовых продуктах, а также транслируем выбор людей в экосистему «Маркетплейса». Будучи крупнейшим в России финансовым супермаркетом, не связанным ни с одной финансовой группой, мы очень хорошо понимаем, что нужно потребителю. В ежедневном режиме Банки.ру анализирует потребительские предпочтения, более 8 млн россиян ежемесячно выбирают с помощью нашего сервиса вклады, кредиты, акции, облигации, страховые полисы, мобильные тарифы из более чем 10 тыс. предложений. Мы знаем, что именно ищут наши клиенты и как удобнее представить информацию для сравнения различных финансовых услуг. Знаем, на что наши клиенты обращают особое внимание, а также какие продукты и сервисы пользуются наибольшим спросом. Знаем почему.

Бизнес-процесс проекта «Маркетплейс» выглядит следующим образом. Человеку необходимо зайти на сайт Банки.ру и пройти аутентификацию через «Госуслуги» (ввести логин и пароль от своего подтвержденного профиля на сайте «Госуслуги). Клиент выбирает финансовый продукт из каталогов. После этого информацию о предпочтении клиента Банки.ру передает Московской бирже.

Московская биржа является технологическим партнером проекта, отвечающим за связь между витриной (Банки.ру) и банками – участниками «Маркетплейса». Все участники проекта в конце апреля 2018 года успешно построили прототип для открытия вкладов в режиме онлайн. Суть прототипа: клиент заходит на Банки.ру, выбирает вклад, который можно открыть онлайн, далее выбирает счет в банке, с которого нужно списать деньги для открытия вклада, и подтверждает желание вводом СМС-кода. Не нужно идти в банк для подписания договора, не нужно идти в другой банк для осуществления банковского перевода. Все это будет сделано автоматически и сэкономит время клиента. По нашим оценкам, процедура открытия вклада будет занимать не более пары минут.

Банки-партнеры получают информацию от Московской биржи о клиенте и о его желании совершить ту или иную операцию. Если возвращаться к прототипу, то Московская биржа передает информацию в банк-донор: с какого счета, какую сумму и куда перевести, а в банк-получатель – какой вклад клиент выбрал, на какую сумму и т. д.

После того как участники трансакций совершат действия для открытия вклада, они передадут информацию в Национальный расчетный депозитарий. НРД подтверждает, что вклад открыт, передает информацию Московской бирже. Банки.ру от биржи получает информацию, что вклад подтвержден со стороны НРД, и транслирует финальный статус для клиента: «Открытие вклада подтверждено». На этом этапе процесс открытия вклада можно считать завершенным.

Этот сервис будет не только про вклады. Как я уже отмечал выше, с помощью «Маркетплейса» можно будет приобрести любые финансовые услуги. Поэтому я считаю, что наш проект даст серьезный импульс развитию финансовых услуг через повышение качества услуг и экономию времени.

Среди преимуществ для банков, страховых и инвестиционных компаний – выход на новые рынки, экономия на содержание филиальной сети и возможность быстрого масштабирования при качественном продукте. С учетом того, что архитектура решения прозрачна и понятна, у финансовых организаций появляется возможность быстрее расти. Выиграют в этой истории банки с хорошим уровнем IT, которые смогут оперативно и без ошибок провести интеграцию с Мосбиржей. Дальнейшие взаимодействия уже происходят между биржей и остальными участниками. На текущий момент – это Банки.ру и Национальный расчетный депозитарий.

Ну и, кроме всего вышесказанного, появление этого проекта усилит конкуренцию между банками, что, по идее, должно привести к повышению качества предоставляемых услуг. Ведь у кредитных организаций не останется такого преимущества, как «шаговая» доступность до офиса».

- **ТАСС – ЦБ сообщил о создании в России трех маркетплейсов финансовых услуг**
  https://tass.ru/ekonomika/5694807

«По словам первого зампреда ЦБ Сергея Швецова, один из них создает Московская биржа

СОЧИ, 19 октября. /ТАСС/. Российские финансовые компании сейчас занимаются разработкой трех маркетплейсов, сообщил первый зампред ЦБ Сергей Швецов на Finopolis.

«Сейчас три маркетплейса готовятся, они могут быть нишевыми, могут конкурировать. Конкуренция – это всегда хорошо, выигрывает тот, кто эффективней, сможет предложить лучший клиентский путь», – сказал он.

«Но это создает определенные трудности, потому что взаимодействие с машиной должно создать другие правила идентификации клиента с точки зрения его риск-профиля и предложения ему правильного набора услуг. Поэтому мы в закон также заложили, что агент, который продает потребителю финансовый продукт, произведенный не им самим, будет нести за него ответственность, как если бы этот продукт продавала сама финансовая организация, которая произвела его», – добавил Швецов.

По его словам, один из маркетплейсов создает Московская биржа, а два другие он отказался назвать.

Позднее советник Швецова Елена Чайковская пояснила ТАСС, что свои маркетплейсы создают «ВТБ Регистратор» и спецдепозитарий «Инфинитум».

«ВТБ Регистратор» будет нишевой платформой для физиков по покупке региональных облигаций. Первый выпуск, который будет предлагаться, – облигации Томской области. Спецдепозитарий «Инфинитум», который подключается к маркетплейсу Мосбиржи в качестве витрины по вкладам, но при этом самостоятельно делает платформу по паевым инвестиционным фондам», – сообщила она.

Накануне глава комитета Госдумы по финансовому рынку Анатолий Аксаков заявил, что законопроект, который будет регулировать работу маркетплейсов, был направлен в профильные ведомства и в ближайший месяц должен быть внесен на рассмотрение Госдумы.

18 октября 21 организация подписала меморандум о вхождении в маркетплейс Московской биржи».

- **Банковское обозрение – Маркетплейс как средство повышения доступности финансовых услуг**
  **https://bosfera.ru/bo/marketpleys-kak-sredstvo-povysheniya-dostupnosti-finansovyh-uslug **

«Проект «Маркетплейс» в настоящее время – один из самых актуальных и ожидаемых на финансовом рынке. Первая презентация его концепции состоялась в октябре 2017 года, запуск проекта – в декабре 2017-го.

МАРКЕТПЛЕЙС И АБР

Решение об участии Ассоциации банков России в реализации проекта по внедрению на финансовом рынке страны национальной системы регистрации финансовых транзакций («Маркетплейс») было принято в январе 2018 года на заседании президиума Ассоциации, в ходе которого первый заместитель председателя Банка России Сергей Швецов выступил с соответствующей инициативой.

Члены Ассоциации активно участвуют в изучении проекта, обсуждении технических вопросов его реализации, а также вошли в рабочую группу по внедрению проекта. Его практическая реализация состоит из трех этапов: создание прототипа и тестовой среды, первой «боевой» версии до изменения законодательства, а затем создание целевой модели, которая будет существовать в измененной нормативной среде.

В настоящее время идет работа над прототипом системы. Рассчитываем, что первая рабочая версия финансового маркетплейса появится в середине февраля 2019 года, а расширенный функционал будет доступен с середины будущего года.

ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

В техническом плане маркетплейс включает в себя платформы для осуществления финансовых транзакций, регистратор финансовых транзакций для учета и подтверждения сделок, витрину для сбора и представления информации о финансовых продуктах (услугах) и ботов (специализированных алгоритмизированных консультантов) для подбора продуктов (услуг) конечным потребителям – физическим лицам.

Платформа – это площадка, на которой взаимодействуют финансовые организации и потребители финансовых услуг в целях заключения финансовых сделок. Основные ее задачи – автоматизация процессов взаимодействия, повышение удобства совершения транзакций, что снимает нагрузку как с потребителя, так и с финансовых организаций.

Агрегатор, или витрина, – автоматизированная платформа, предоставляющая потребителю финансовых услуг возможность выбора финансового продукта посредством систематизации и визуализации финансовых услуг в определенной последовательности, зависящей от заданных критериев (параметров). Это могут быть как списки, сортированные по заданным параметрам, так и специальные рэнкинги (например, народные рейтинги банков).

Бот – это автоматизированная система, которая предоставляет посредством использования определенных алгоритмов и технических средств консультации в отношении финансовых услуг, сервисы по заключению и исполнению финансовых сделок.

СВОЕВРЕМЕННОСТЬ И НЕОБХОДИМОСТЬ

Маркетплейс представляет собой новую систему дистанционной продажи финансовых продуктов. Новая инфраструктура будет соединять продавцов (банки, страховые и иные финансовые компании) и потребителей. Она сможет заменить или дополнить традиционные каналы продаж – офисы, сайты, мобильные приложения отдельных компаний. Вместо этого потребители смогут приобретать финансовые продукты через сайты и мобильные приложения витрин-агрегаторов, которые показывают информацию от многих продавцов и дают возможность сравнить финансовые продукты. Например, через приложение в мобильном телефоне можно будет сравнить процентные ставки по банковским вкладам разных банков, выбрать вклад и тут же открыть его.

Создание маркетплейса, на наш взгляд, обусловлено необходимостью повышения финансовой доступности услуг, формирования безопасной, доверенной среды для финансовых транзакций.

Маркетплейс призван, с одной стороны, обеспечить равный доступ пользователей услуг к финансовому рынку, с другой – сформировать предпосылки для развития

конкурентной среды и оптимизации финансовых сервисов. Среди преимуществ проекта – улучшение ситуации с финансовой доступностью, в частности, за счет снятия географических ограничений. При этом пользователи получат дистанционный доступ к финансовым услугам в режиме 24/7 и широкую линейку финансовых продуктов. Еще одним преимуществом для пользователей станет оптимизация процесса возмещения средств физическим лицам по вкладам, договора по которым заключены в системе, в случае отзыва (аннулирования) лицензии у банка.

В настоящее время, выбрав желаемый продукт, люди вынуждены переходить с сайта агрегатора на интернет-страницу соответствующего банка, в большинстве случаев идти в его отделение для получения необходимых услуг. С маркетплейсом это не потребуется. Его задача – облегчить действия, которые приходится совершать клиенту и его банку в повседневной жизни.

Мы уже привыкли получать многие услуги в одном окне, то же нас ждет и на финансовом рынке. Это приведет к изменению привычного алгоритма обращения к услугам финансовых организаций.

ПРОДУКТОВАЯ ЛИНЕЙКА

Данный проект направлен прежде всего на обеспечение потребностей клиентов, позволит повысить уровень доступности и качества услуг, удовлетворенности потребителей, в том числе за счет широкого спектра услуг, предлагаемых разными компаниями. Если раньше в отдаленных регионах страны выбор потребителей ограничивался кругом финансовых организаций, предоставляющих услуги в конкретном регионе, то теперь граждане смогут выбирать из широкого числа поставщиков услуг.

Создание маркетплейса, на наш взгляд, обусловлено необходимостью повышения финансовой доступности услуг, формирования безопасной, доверенной среды для финансовых транзакций

Продуктовый ассортимент маркетплейса будет включать вклады, государственные и корпоративные облигации, страховые продукты. В перспективе он может быть расширен за счет кредитных, инвестиционных и прочих финансовых продуктов. Безусловно, работа с этими продуктами отвечает запросам членов Ассоциации банков России.

Полагаю, что проект «Маркетплейс» даст серьезный импульс развитию финансовых услуг через повышение качества услуг и экономию времени.

Участники Ассоциации банков России высоко оценивают потенциал данного проекта для развития конкуренции и собственного бизнеса.

КОНКУРЕНЦИЯ И ЗАРУБЕЖНЫЙ ОПЫТ

Появление этого проекта усилит конкуренцию между банками. Региональные компании смогут конкурировать с крупными игроками на равных условиях.

По мнению участников Ассоциации, среди преимуществ для банков, страховых и инвестиционных компаний – выход на новые рынки, экономия на содержании филиальной сети и возможность быстрого масштабирования при качественном продукте.

Мы видим заинтересованность в участии в данном проекте со стороны многих банков. В настоящее время в рабочую группу по реализации проекта «Маркетплейс» входят

Московская биржа и Национальный расчетный депозитарий, которые будут отвечать за инфраструктуру маркетплейса, две витрины маркетплейса – «Банки.ру» и Fins, а также пять кредитных организаций – участников Ассоциации банков России: «Ак Барс», «Центр-инвест», «Зенит», Совкомбанк и Росбанк.

Участники проекта активно задействованы в разработке и тестировании технических, бизнес- и юридических решений на этой платформе.

По оценкам Банка России, пользователями финансового маркетплейса могут стать несколько десятков миллионов людей в первые три года работы.

Стоит отметить, что в сфере создания маркетплейсов Россия – в общемировом тренде. В Европе распространены финансовые маркетплейсы, однако это чаще площадки, сфокусированные на одном направлении услуг. Например, немецкие сервисы Raisin и Deposit Solutions занимаются управлением активами, портал Zillow агрегирует и предлагает ипотечные кредиты. В Китае также работает масштабный кредитный маркетплейс Lu.com, который выдает в режиме онлайн потребительские кредиты.

В России отрасль финансовых технологий во многом следует мировым тенденциям. Российской особенностью в этой сфере является то, что в отличие от зарубежного опыта у нас ведущие банки и финансовые компании зачастую реализуют наиболее интересные решения и сами модернизируют традиционные финансовые услуги. В то же время появляется много новых высокотехнологичных компаний, а вместе с ними и наиболее передовые технологии, что способствует увеличению конкуренции в отрасли. Развитие финансового рынка невозможно представить без внедрения и развития финансовых технологий. Банки и финансовые организации становятся более технологичными, в результате чего у них появляется возможность предоставлять более надежные, безопасные и качественные услуги населению, поэтому финансовые технологии в России, определенно, продолжат свое развитие.

КАК ЭТО РАБОТАЕТ

Бизнес-процесс проекта на примере «Банки.ру» выглядит следующим образом. Человеку необходимо зайти на сайт «Банки.ру» и пройти аутентификацию через сервис «Госуслуги» (ввести логин и пароль от своего подтвержденного профиля на этом сайте). Клиент выбирает финансовый продукт из каталогов, например вклад, который можно открыть онлайн. Далее выбирает счет в банке, с которого нужно списать деньги для открытия вклада, и подтверждает желание вводом СМС-кода. Не нужно идти в банк для подписания договора, не нужно идти в другой банк для осуществления банковского перевода. Все произойдет автоматически и сэкономит время клиента. По оценкам «Банки.ру», процедура открытия займет не более пары минут.

После этого информацию о предпочтении клиента «Банки.ру» передает Московской бирже. Она передает информацию в банк-донор – с какого счета, какую сумму и куда перевести, а в банк-получатель – какой вклад клиент выбрал, на какую сумму и т. д.

Таким образом, банки-партнеры получают информацию от Московской биржи о клиенте и его желании совершить ту или иную операцию.

По оценкам Банка России, пользователями финансового маркетплейса могут стать несколько десятков миллионов людей в первые три года работы

После того как участники трансакций совершат действия для открытия вклада, они передадут информацию в Национальный расчетный депозитарий (НРД). НРД подтвердит, что вклад открыт, передаст информацию Московской бирже. «Банки.ру» от биржи получит информацию, что вклад подтвержден со стороны НРД, и транслирует финальный статус для клиента: «Открытие вклада подтверждено». На этом этапе процесс открытия вклада можно считать завершенным.

Московская биржа фактически представляет IT-платформу, которая является посредником между витринами (финансовыми супермаркетами), клиентом и финансовой организацией. В течение реализации пилотного проекта трансакции будет проводить ограниченное число банков, но с полноценным функционалом, включая регистрацию трансакций с использованием юридической и тарифной моделей. Затем в течение двух-трех месяцев проект будет выведен на полную мощность, тогда любые участники смогут подключаться к платформе.

Важным звеном в цепочке, обеспечивающей безопасность всех операций, станет регистратор финансовых трансакций. Он представляет собой систему хранения данных о заключенных сделках. По запросу клиенту будут предоставляться выписки из реестра для использования в качестве юридически значимой информации (например, в судах), также клиент сможет видеть информацию по всем заключенным сделкам в своем личном кабинете по принципу «одного окна». Планируется, что такой личный кабинет будет находиться на сайте «Госуслуги». Например, в личном кабинете можно будет получить информацию о своих вкладах, размещенных в разных банках.

Таким образом, маркетплейс позволит потребителям видеть все свои операции, финансовые продукты, историю взаимодействия с банками и страховщиками в «одном окне». Пользователь сможет более эффективно вести личный финансовый учет, защищать свои права в судебных спорах и т.д. Кроме того, это поможет снизить риск забалансовых вкладов в банках.

РЕГУЛЯТОРНАЯ ПОДГОТОВКА

Сразу замечу, что реализация проекта «Маркетплейс» не предполагает государственных инвестиций, ее построение будет происходить на рыночных принципах. И то, что к платформе подключились уже несколько крупных банков, говорит об интересе и доверии к этому проекту со стороны участников рынка.

Другое дело, что для полноценной работы финансового маркетплейса в России потребуется соответствующее изменение законодательства. В частности, нужно принять законы о регистраторе финансовых операций, о финансовом агрегаторе, а также нормативные акты о продуктах и ответственности разработчиков ботов.

В этой связи задачу Банка России мы видим в создании нормативной базы для эффективного функционирования такой системы. Подготовке нормативного регулирования будут способствовать опыт пилотного запуска системы и анализ бизнес-моделей ее участников.

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Проект «Маркетплейс» станет своего рода вызовом для российских финтех-разработчиков. Не исключаю, что в перспективе возможна интеграция услуг Robo-advisors.

Привычная форма создания инвестиционного портфеля посредством общения с финансовым консультантом в робоэдвайзинге заменяется программным алгоритмом. Существующие платформы, которые уже умеют определять потребности клиента и его склонность к риску, формировать, исходя из этих данных, инвестиционный портфель. Роль самого инвестора сводится к контролю за работой сервиса, при этом наиболее важные операции, например, покупка ценных бумаг на бирже, обязательно проходят ручную верификацию специалиста. Подобный сервис помогает накопить на крупные покупки, сохранить накопления, а также позаботиться о собственной пенсии».

- **ЭкспертONLINE – ЦБ создал маркетплейс с функциями мониторинга** **http://expert.ru/2017/12/20/marketplejs-tsentrobanka-budet-i-nedryomannyim-okom/**

«Клиенты будут следить за финансистами, а ЦБ – за всеми в рамках создаваемого главным банком маркетплейса. Контроль за активами и транзакциями граждан в режиме онлайн будет доступен как им самим, так и Центральному банку. Впрочем, если вам нечего скрывать, кроме своей банковской тайны, про которую вспоминают все реже, возможность мониторинга может оказаться очень полезной.

В чем смысл

Как заявил советник первого зампреда ЦБ Сергея Швецова Степан Кузнецов на Международном репо-форуме, регулятор уже определил приоритетные направления, которые будет развивать для граждан в создаваемом им маркетплейсе. Первыми финансовыми инструментами, за которыми проследит Банк России в рамках системы контроля за транзакциями российских граждан, станут вклады, ОФЗ и ОСАГО.

«Первый инструмент – вклады. Он наиболее востребованный и позволит всю систему архитектуры маркетплейса выстроить. Следующая история ОФЗ. Понятно, что есть идеи разобраться с ОСАГО как обязательным видом страхования, с которым много проблем. В этом вопросе у нас плотное взаимодействие с Российским союзом автостраховщиков. Вот это три направления, в которых мы движемся. В дальнейшем все зависит от запроса рынка», – передает агентство ТАСС слова Степана Кузнецова.

Он напомнил, что смысл маркетплейса заключается в том, чтобы граждане могли в режиме онлайн видеть свои вклады, список приобретенных ценных бумаг и выбрать компанию для оформления полиса ОСАГО. Маркетплейс создается одновременно с системой регистрации всех финансовых транзакций россиян – об этой системе Швецов объявил в начале октября. По замыслу ЦБ единая система регистрации финансовых транзакций россиян позволит потребителю видеть все свои операции в одном месте и использовать эти данные при спорах в суде, а также избежать проблемы забалансовых вкладов в банках.

Полная прозрачность

Эта площадка формируется федеральным правительством и формально будет выполнять функции портала госуслуг по информированию населения о существующих у них деньгах у любого отечественного участника финансового рынка, поясняет директор развития агентской сети УК «Солид Менеджмент» Сергей Звенигородский. На начальном этапе администрирование коснется только банковской сферы и всех вкладов в них. Система

позволит ЦБ наиболее полно отслеживать как активность самого человека, так и банка, которому придется все операции с клиентами проводить под контролем ЦБ.

Вторым направлением будет подсчет активов в руках граждан, что также служит двоякой цели – учесть полную налоговую базу и отслеживать активность участников с ценными бумагами. ОФЗ отследить наиболее просто, все данные есть у Минфина и профучастников, которые в свою очередь постоянно отчитываются перед ЦБ. С другими ценными бумагами дело будет продвигаться уже на базе созданного базиса по ОФЗ и через несколько лет полная база по отечественному размещению активов и банковских вкладов будет дополнительным подспорьем как в судах (вернуть деньги при банкротстве или наследовании), так и для налоговой службы.

Создание подобного портала для ОСАГО позволит учесть реальные полисы и отсечь рынок нелегальных, чтобы каждый автовладелец и представитель ГИБДД мог оперативно определить законность документа, уверен Сергей Звенигородский.

Усилить физическое лицо

Начинание Центробанка о едином маркетплейсе – крупный шаг вперёд в упорядочивании финансовых инструментов людей, полагает ведущий аналитик ГК TeleTrade Марк Гойхман. Физическое лицо – изначально более слабая сторона во взаимоотношениях с банками, страховыми компаниями, институциональными участниками рынка. Единая система регистрации и информации сделок людей на финансовых рынках повышает надёжность, юридическую защищённость человека в данных сферах.

Маркетплейс не является альтернативой торговым площадкам, в частности, МосБирже, констатирует эксперт. Здесь не совершаются сделки, а фиксируются и получают дополнительное подтверждение те, которые заключены гражданином с разными институтами. Для человека это его своеобразный «бэк-офис», по аналогии со службой оформления и регистрации сделок финансовой компании. Это тем более важно в связи с тем, что мейнстрим современного развития – дистанционное предоставление услуг, зачастую безбумажное.

Гражданин, оформивший вклад, купивший ОФЗ, полис ОСАГО, может получить юридическое удостоверение данных фактов в одном месте. Вместо разрозненных элементов информации по отдельности с каждым контрагентом, появляется единая целостная система фиксации отношений человека с рынком. Это качественно повышает доверие людей к нему, будет способствовать привлечению личных инвестиций в денежный оборот, развитию более сложных инструментов. Исчезает, в частности, болезненная проблема забалансовых вкладов в банках.

Причём потребители системы – не только граждане, напоминает Марк Гойхман. Такая практика нужна им для взаимоотношений и с банками по кредитам, с налоговой службой, госуслугами. В маркетплейс, по его словам, есть смысл впоследствии добавить данные по приобретённым акциям, паям ПИФов, корпоративным и региональным облигациям, ИИС, личному и имущественному страхованию. Можно объединить базу с данными по госрегистрации личной недвижимости, автотранспорта, залогов».

Не так давно предлагались также иные способы решения проблемы обеспечения достоверности вкладов:

- **Известия – Вкладчиков запомнят навеки**
  https://iz.ru/719470/anastasiia-alekseevskikh/vkladchikov-zapomniat-naveki

«Банк России занесет всех клиентов кредитных организаций в блокчейн

В России появится единый реестр вкладчиков на базе технологии блокчейн – его в следующем году создадут Центробанк и Агентство по страхованию вкладов (АСВ). Об этом «Известиям» рассказали источники, близкие к АСВ и ЦБ, и подтвердили два банкира, знакомых с ситуацией. Пока в мире нет аналогов создаваемому реестру депозитов. Его внедрение поможет бороться с недобросовестными банкирами, уничтожающими базы данных клиентов в момент отзыва лицензии. По словам экспертов, нововведение повысит прозрачность рынка банковских депозитов.

При открытии депозита информацию об этом кредитная организация будет записывать в блок реестра, который будет храниться на сервере ЦБ, рассказал источник, близкий к Банку России. В каждом блоке будет храниться информация о названии банка, персональные данные вкладчика и сумма депозита. При пополнении или закрытии вкладов изменения будут записываться в новый блок реестра.

Данные из блокчейн-реестра нельзя изменить или удалить, поэтому вся информация о вкладчиках будет надежно защищена, отметил источник, близкий к АСВ. Таким образом, использование технологии блокчейн поможет избежать ситуаций, когда при отзыве лицензии банки «теряют» базы данных вкладчиков, которые из-за этого не могут получить страхового возмещения, полагающегося им по закону.

Источник, близкий к ЦБ, отметил, что пока неясно, будет ли использована сторонняя технология на основе блокчейн или создана собственная.

В ЦБ и АСВ на запросы «Известий» не ответили.

В мире нет аналогов создаваемому реестру вкладчиков, отметила управляющий партнер аудиторской компании «2К» Тамара Касьянова.

СПРАВКА «ИЗВЕСТИЙ»

Блокчейн (от английского blockchain – «блочная цепь») – это технология хранения и защиты информации с помощью распределенных баз данных.

Первый замгендиректора АСВ Валерий Мирошников ранее рассказывал «Известиям», что «сотрудники ЦБ и АСВ не раз сталкивались с ситуацией, когда за три дня банк-«мертвец» успевал уничтожить базы данных или вывезти их за пределы кредитной организации». Например, в банке «Холдинг-Кредит», который лишился лицензии в 2013 году, сервер якобы разбили переносившие его таджики-рабочие – на самом деле он был вывезен накануне отзыва лицензии, а временной администрации подкинули муляж. Поиски оригинального сервера заняли десять месяцев. В Международном промышленном банке экс-сенатора Сергея Пугачева сотрудники по указанию руководства занимались уничтожением баз данных каждые три месяца, приводил еще один пример Валерий Мирошников.

– Система страхования банковских вкладов сыграла очень важную роль. Введение реестра станет следующим шагом для обеспечения стабильности на рынке вкладов, так как

эта мера не позволит недобросовестным банкирам уничтожать данные о клиентах, – отметил управляющий директор по розничным продуктам Абсолют-банка Антон Павлов.

Применение технологии блокчейн позволит ЦБ получать не только общую информацию об объемах вкладов в банках, но и четко отслеживать в режиме реального времени данные о каждом открытом или закрытом депозите, отметил член экспертного совета по цифровой экономике и блокчейн-технологиям при Госдуме Никита Куликов. Система распределенного реестра позволит Банку России структурировать данные о депозитах физлиц, например, отслеживать изменения спроса на типы вкладов, добавил президент банка «Воронеж» Олег Кисляк.

Сама по себе технология блокчейн отвечает за наличие записей в реестре, а насколько они верные и безошибочные – это уже вопрос к операторам, то есть банкам, которые и будут вносить информацию, отметил Никита Куликов. К тому же по-прежнему останется нерешенной проблема «забалансовых вкладчиков», которая связана с тем, что информация о людях, доверивших банкам деньги, просто не вносилась в отчетность, добавил он.

Создание Банком России и АСВ единого реестра будет способствовать развитию рынка вкладов в России. Клиенты станут охотнее открывать депозиты: зная, что их данные будут дополнительно защищены, они с большей уверенностью смогут рассчитывать на страховое возмещение в случае банкротства банка. По данным ЦБ, объем рынка вкладов за прошлый год вырос на 7,4% и достиг 26 трлн рублей к 1 января 2018 года».

- **Banki.ru – ЦБ планирует запустить единый реестр вкладов физлиц** **https://www.banki.ru/news/lenta/?id=10492854**

«В ЦБ пришли к выводу, что единый реестр вкладов физлиц необходим

Центральный банк планирует запустить единый реестр вкладов физических лиц, который объединит данные по банковским вкладам российских граждан. Об этом рассказала председатель Банка России Эльвира Набиуллина на конференции Международной ассоциации страховщиков депозитов.

«В процессе очищения банковской системы нам пришлось столкнуться с вопиющими случаями забалансовых вкладов. Их было не так много, если сравнивать с общим числом вкладчиков и объемами вкладов в системе, но мы считаем эту проблему достаточно серьезной. Она затрагивает интересы граждан, которые попадают в очень серьезную ситуацию. Здесь нужно выработать специальные решения. Мы долго обсуждали и планируем все-таки запустить единый реестр вкладов физических лиц, которые объединит данные по банковским вкладам граждан РФ», – рассказала глава регулятора в ходе выступления.

«Это серьезный технологический проект, который, мы уверены, будет способствовать повышению доверия вкладчиков и ответственному поведению менеджмента банка», – подчеркнула она.

О том, что Банк России рассматривает вопрос введения единого реестра вкладчиков для борьбы с забалансовыми вкладами, год назад говорил зампред регулятора Дмитрий Тулин.

В марте «Известия» писали, что единый реестр вкладчиков на базе технологии блокчейн появится в 2019 году. Предполагается, что при открытии депозита информацию об этом кредитная организация будет записывать в блок реестра. В каждом блоке будут храниться информация о названии банка, персональные данные вкладчика и сумма депозита. При пополнении или закрытии вкладов изменения будут записываться в новый блок реестра.

Данные из блокчейн-реестра нельзя изменить или удалить, поэтому вся информация о вкладчиках будет надежно защищена. Таким образом, использование технологии блокчейн поможет избежать ситуаций, когда при отзыве лицензии банки «теряют» базы данных вкладчиков, которые из-за этого не могут получить страхового возмещения, полагающегося им по закону.

По словам экспертов, применение технологии блокчейн позволит ЦБ не только получать общую информацию об объемах вкладов в банках, но и четко отслеживать в режиме реального времени данные о каждом открытом или закрытом депозите».

5. Кейс «Незаконное списание средств с банковской карты при оплате услуг через интернет»

Вопросы безопасности использования электронных средств платежа очень активно обсуждаются в популярной и в специальной литературе, в интернет-форумах.

На официальном сайте Банка России (http://www.cbr.ru/PSystem/) опубликованы статистические и аналитические материалы о развитии рынка платежных услуг (раздел «Наблюдение в национальной платежной системе»), нормативные документы и разъяснения к ним (в виде вопросов и ответов) (раздел «Регулирование в национальной платежной системе»), памятка о мерах безопасности при использовании банковских карт.

Рекомендуем обратиться к нашему Комплекту аннотированных материалов для участников Олимпиады по финансовой грамотности для студентов бакалавриата и специалитета (Москва, 2018)**,** на сс. 219-265 которого представлены материалы по кейсу «Несанкционированное списание денежных средств», в том числе материалы по проблемам защиты прав потребителей-держателей банковских карт. Сборник доступен по ссылке https://fingramota.econ.msu.ru/competition/lib/2017-2018/4students.

5.1. Обзоры и консультации о мерах безопасности при дистанционной оплате товаров и услуг

Материалов о мерах безопасности при совершении финансовых операций в сети много, но к сожалению, они всегда актуальны. Насколько они полные – судить Вам.

Служба поддержки Яндекса опубликовала следующий материал:

- **Яндекс – Мошенничество в сети**
  https://yandex.ru/support/common/security/phishing.html

«В интернете можно столкнуться с мошенниками, цель которых – завладеть личной информацией пользователя. Личные данные – это фамилия, имя, отчество, пароли от учетных записей к социальным сетям, паспортные данные, реквизиты банковской карты и другие личные сведения.

Личная информация нужна для полноценной работы многих приложений и сайтов. Например, вы указываете ФИО и адрес при оформлении заказа в интернете или электронную почту – при подписке на рассылку.

Мошенники используют незаконно полученную информацию, чтобы рассылать спам или получить доступ к вашему мобильному или банковскому счету. Поэтому важно распознать подозрительный или ненадежный сайт, прежде чем вводить личные данные.

Стоит ли передавать информацию конкретному сайту, решать вам. Лучше не оставлять личные данные на подозрительных сайтах.

Способы хищения данных

Злоумышленники используют разные схемы хищения личной информации.

Фишинговые сообщения

Фишинговые сообщения – это письма от мошенников, которые представляются банками и другими официальными организациями. Цель таких писем – заставить вас ввести пароль или данные карты в поддельную форму.

Злоумышленники запрашивают конфиденциальные данные для подтверждения учетной записи или активации почтового ящика. В результате ваша личная информация оказывается у мошенников.

Примеры

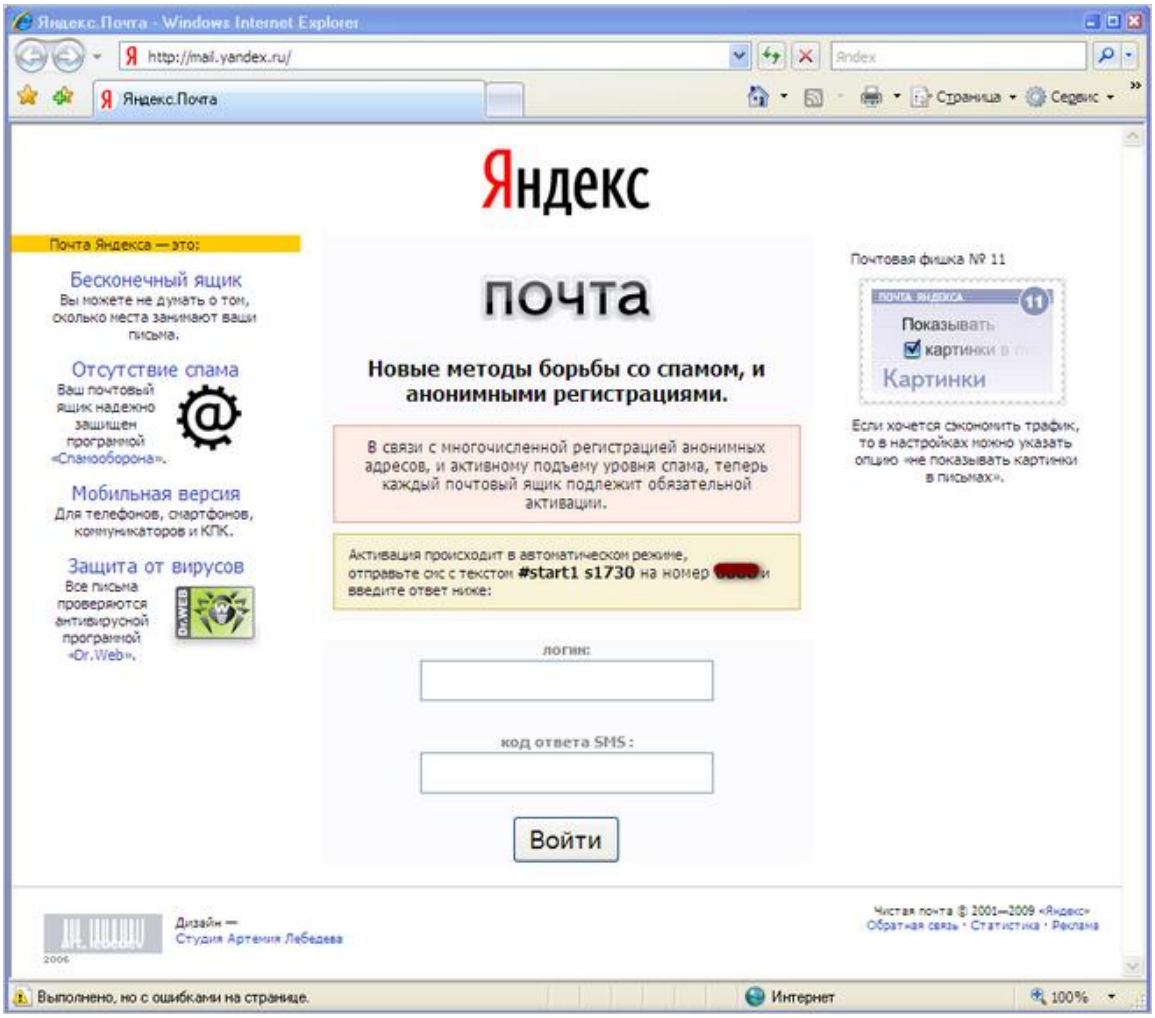
Поддельные сайты

Подмена сайта – это скрытое перенаправление пользователей на поддельные сайты с помощью вредоносных программ. Пытаясь зайти на популярный сайт, пользователь попадает на сайт-подделку, очень похожий на оригинал. Данные учетной записи, введенные на таком сайте, оказываются у злоумышленников.

Чтобы распознать сайт-подделку, обратите внимание на адрес в поисковой строке – он будет отличаться от официального. В правом верхнем углу вы не найдете значка безопасного соединения, а размещенные на поддельной странице ссылки, скорее всего, будут нерабочими.

Примеры

Пример подмены сайта:



Подмена сайта происходит по двум сценариям:

- Вирус искажает информацию о домене в системе DNS. Для настройки DNS воспользуйтесь бесплатным сервисом Яндекс.DNS.

- Вирус меняет системный файл hosts на вашем компьютере. Проверьте компьютер антивирусной утилитой CureIt! от Dr.Web или Virus Removal Tool «Лаборатории Касперского».

Телефонное мошенничество

Телефонные мошенники звонят или рассылают SMS от имени банка или платежной системы с просьбой предоставить номер карты или перевести деньги на указанный номер. Причины могут быть разными: истекший срок действия пароля, блокировка карты, крупный выигрыш или даже авария с участием близкого человека.

Вас могут попросить перейти по ссылке для восстановления доступа к аккаунту, отправить SMS или позвонить по конкретному номеру. Цель таких сообщений – списать деньги за отправку ответного SMS, подписать на платные услуги или заставить вас ввести пароль и данные карты.

Примеры

Мошенничество в социальных сетях

Мошенники в соцсетях рассылают сообщения с предложением приобрести товар с большой скидкой или получить выигрыш за предоплату. Цель таких сообщений – убедить вас отправить деньги.

Примеры

Внимание. Существуют и другие способы хищения информации, поэтому будьте внимательными, когда сообщаете сведения о себе – мошенники могут этим воспользоваться.

Рекомендации по защите данных

1. Не оставляйте незаблокированными телефоны и компьютеры, не выбрасывайте бумаги и носители данных (жесткие диски, SIM-карты, flash-карты), на которых хранятся пароли.
2. Если компьютером пользуется несколько человек, используйте разные профили операционной системы.
3. Не храните в электронной почте и не выкладывайте в открытый доступ копию документов, удостоверяющих личность: если мошенники взломают вашу почту, они смогут воспользоваться личными данными.
4. Перед работой на чужом компьютере войдите в приватный режим. Если такой возможности нет, очистите кэш, и cookie после завершения работы.
5. Регулярно проверяйте антивирусом съемные диски, флеш-карты и прочие носители информации, которые вы подключаете к чужим компьютерам.
6. Не вводите личную информацию в подозрительные формы, особенно в электронных письмах.
7. Не открывайте вложения и не переходите по ссылкам из электронной почты или мессенджеров (Telegram, WhatsApp и т. п.) от сомнительных адресатов. Если адресат кажется вам подозрительным, внесите его в черный список.
8. Позвоните по официальному номеру банка или другой организации, от имени которой было отправлено подозрительное письмо.

9. Прежде чем совершать покупки онлайн, проверяйте отзывы и рейтинг магазинов, аккаунты продавцов и условия оплаты.
10. Оплачивайте покупки только через известные платежные сервисы и системы (например, Яндекс.Деньги, Visa, WebMoney, Paypal) – такие платежи надежно защищены.
11. Выбирайте сайты с протоколом https, а не http: вероятность взлома сайтов с http гораздо выше, чем сайтов с https.
12. Прежде чем вводить логин и пароль на сайте, убедитесь, что в адресной строке браузера указан верный адрес. Фишинговые веб-страницы могут иметь адрес, очень похожий на настоящий (например, yanclex.ru вместо yandex.ru).
13. Закройте страницу, если в браузере появится сообщение о переходе на подозрительный сайт. Яндекс.Браузер, например, использует панель Protect, отслеживая мошеннические сайты.
14. Подключите двухфакторную аутентификацию для всех своих аккаунтов.

Подробнее о безопасности в сети читайте в разделе Помощи.

Если вы стали жертвой мошенников

- Если с вашего счета незаконно списали денежные средства, заблокируйте карту по телефону и обратитесь в полицию.
- Если вы отправляли SMS на короткий номер, указанный мошенниками, попытайтесь вернуть деньги через мобильного оператора или компанию, которой принадлежит этот номер.
- Если вы перешли по фишинговой ссылке, проверьте ваш компьютер на вирусы, например, с помощью бесплатных антивирусных программ.
- Если вы ввели пароль на поддельной странице, смените пароль, контрольный вопрос и ответ на него после проверки на вирусы.
- Если вы ввели пароль на поддельной странице вашего аккаунта на Яндексе, измените пароль, секретный вопрос и ответ на него в Паспорте. Если доступ к аккаунту потерян, воспользуйтесь инструкцией по восстановлению доступа».

Обзорные материалы и рекомендации по защите платежей, опубликованные в СМИ:

- **Forbes – Безопасность в интернете: как защитить свои платежи? http://www.forbes.ru/finansy-i-investicii/346943-bezopasnost-v-internete-kak-zashchitit-svoi-platezhi**

«Наверное, не существует ни одного активного пользователя интернета, который ни разу что-нибудь не купил или не оплатил онлайн. И каждый раз, вводя данные своей банковской карты, человек подвергается потенциальной опасности

В 2016 году объем незаконных операций с банковскими картами составил около 1 млрд рублей, сказал недавно первый заместитель председателя Банка России Георгий Лунтовский. Эта цифра уменьшается по сравнению с прошлыми годами благодаря развитию систем защиты. Но, к сожалению, масштаб мошенничества все еще очень велик.

В качестве примеров можно привести один из участившихся случаев мошенничества – поддельные страницы сайтов. Например, потенциальный клиент

хочет приобрести электронный полис ОСАГО. Поиск выдал ему поддельную страницу. Пользователь выбирает услугу и заполняет платежные реквизиты. Все данные карты сразу попадают к мошеннику, который в то же время вводит их на другом реальном ресурсе, но предназначенном, например, для перевода денежных средств или пополнения услуг связи. Проверочный код пользователь также передает мошеннику, но денежные средства в результате оказываются в кармане у последнего. Этот вид мошенничества называется «фишинг». Его и многие другие виды мошенничества можно избежать, постоянно обращая внимание на детали и следуя алгоритму, описанному ниже.

В безопасности интернет-операций заинтересованы не только держатели карт, но и банки, интернет-магазины и платежные системы, которые разрабатывают все новые, более совершенные и одновременно дорогостоящие средства безопасности онлайн-платежей и защиты от мошенников. Все участники транзакции рискуют своими деньгами, а магазины, банки и системы – еще и своей репутацией.

Какие существуют современные меры безопасности интернет-платежей, кто и за что отвечает непосредственно во время транзакции и как избежать мошенников во всемирной паутине?

Кто здесь главный?

В каждом процессе платежа принимает участие несколько сторон. Одна сторона – это держатель карты, физическое лицо, совершающее операцию. Другой стороной является интернет-магазин или любая другая торговая площадка, которая предлагает товары или услугу. Между ними стоят банк-эмитент и банк-эквайер. Первый – тот, кто выдал вам карту, на счету у которого находятся деньги. Второй – это банк, который производит данную финансовую операцию. В некоторых случаях роль эмитента и эквайера может играть один и тот же банк. Последними, но не менее важными участниками операции выступают международные платежные системы и сервис-провайдеры – они осуществляют процессинг операции.

Когда вы совершаете покупку в интернет-магазине и нажимаете кнопку «Оплатить», вы переходите на страницу платежной формы для заполнения необходимых данных. Далее платежная система (сервис-провайдер) передает все ваши данные в банк-эквайер, который обслуживает этот интернет-магазин. Банк-эквайер, в свою очередь, передает информацию банку-эмитенту, который выпустил и выдал вам карту. Последний проверяет информацию о вас, о карте, наличии свободных средств на ней, иногда запрашивая авторизацию покупателя по технологии 3-D Secure, о которой мы подробно расскажем далее. После этого он разрешает (или не разрешает) провести операцию, передает данные платежной системе, платежная система – в магазин, а покупателю приходит уведомление, что операция совершена.

А кто отвечает за безопасность?

За безопасность интернет-операции отвечают все, кто принимает в ней участие. Ответственные банки, интернет-магазины, платежные системы постоянно совершенствуются, изобретая все новые способы обезопасить себя и своего клиента от возможной угрозы. На сегодняшний момент существует ряд протоколов и правил, о

которых вам как непосредственным участникам любой транзакции необходимо знать и помнить каждый раз, когда вы совершаете онлайн-платеж.

Протокол SSL – Secure Socked Layer. Он позволяет безопасно передавать зашифрованную информацию от пользователя к серверу. Сайты, использующие SSL, передают зашифрованные данные по протоколу HTTPS, расшифровать которые можно с помощью специального секретного ключа. Это отличает их от незащищенных сайтов, использующих обыкновенный протокол HTTP.

Стандарты PCI DSS (Payment Card Industry Data Security Standard). Эти стандарты защиты информации, разработанные международными платежными системами, защищают данные банковских карт. Любая компания, которая собирается осуществлять интернет-платежи, должна соответствовать стандартам PCI DSS. Например, международная платежная система Visa с 2006 года обязывает всех, кто ее использует, ежегодно проходить проверку на соответствие этим стандартам.

Технология 3-D Secure. Важная ступень защиты – проверка личности держателя карты в реальном времени, которую включает банк-эмитент. Обычно такая проверка проходит при помощи СМС. После ввода номера карты ее владелец перенаправляется на сервер своего банка-эмитента. Обычно в качестве подтверждения банк отправляет покупателю СМС с секретным кодом. При введении присланного кода вы подтверждаете свою личность, после чего банк разрешает проведение транзакции. Например, система MasterCard использует систему MasterCard Securecode при подтверждении каждого онлайн-платежа.

Платежная система авторизует и идентифицирует покупателя. Такие крупнейшие системы, как PayPal или Apple Pay, сами авторизуют и идентифицируют клиента. Клиент не должен каждый раз заново вводить платежные данные – это снижает риск утечки информации о банковской карте.

Антифрод-системы. Дословно это переводится как «противомошеннические». Это системы-платформы, которые оценивают финансовые операции онлайн и способны обнаружить сомнительные. Они могут предотвратить списание денег, если есть подозрение на мошенничество. Каждая операция, проходя через платформу, анализируется, после чего дается рекомендация отклонить или применить дополнительную проверку.

Антифрод-системы могут работать по разным параметрам: лимиты по совершению операций с одного IP-адреса, ограничение по сумме, времени или количеству покупок, а также постоянно меняющийся алгоритм, оценка поведения покупателя в процессе платежа, транзакции на основе статистики и др. Система оценивает операции и выявляет аномальные и подозрительные. Современные антифроды способны с максимальной степенью вероятности опознать мошенника или определить операции покупателей как доверенные и не проводить дополнительную авторизацию платежа по СМС. Это, безусловно, повышает удобство для покупателя и способствует продвижению интернет-магазинов.

Что делать?

Рассмотрев и изучив все меры безопасности, которые принимают интернет-магазины, банки и платежные системы, разработайте свой алгоритм действий. Другие участники операции принимают повышенные меры безопасности, но и сам пользователь не

должен их нарушать, обходить или невнимательно к ним относиться. Иначе все попытки вас обезопасить будут абсолютно бесполезны.

Ответственно подходить к совершению транзакций через интернет, выработать у себя минимальные навыки для обеспечения онлайн-безопасности – это главные элементы современной финансовой грамотности, соблюдать которую следует всем интернет-пользователям.

1. Подключите интернет-банк и СМС-оповещение. Это позволит вам отслеживать операции в режиме реального времени.
2. Не используйте подозрительные сайты. Адрес защищенного сайта должен начинаться с https://. Также рядом с адресной строкой должна быть иконка в виде закрытого замка. Эти знаки покажут, что вы имеете дело с ответственным продавцом и ваши данные будут передаваться в зашифрованном виде.
3. Используйте 3-D Secure – авторизацию платежа по СМС, при этом обращайте внимание на назначение платежа, которое приходит в СМС от банка вместе с проверочным кодом.
4. Ищите на сайте надпись Verified by Visa или MasterCard Securecode – в зависимости от того, какой платежной системой вы пользуетесь. Сайты, которые размещают у себя такие логотипы, будут соответствовать стандартам PCI DSS и/или использовать технологию 3-D Secure.
5. Откройте отдельную карту для интернет-платежей и не храните на ней значительных денежных остатков.
6. Не сообщайте данные своей банковской карты другим людям: ни банковским служащим, ни работникам интернет-магазинов.
7. Если интернет-магазин по каким-либо причинам вызывает у вас подозрение, используйте платежные системы Apple Pay, PayPal или другие. В этом случае вам не нужно будет делиться данными своей банковской карты.
8. Совершайте покупки с устройств, на которых установлена антивирусная защита. Операционная система iOS (все устройства Apple) не требует специальных антивирусов. Каждое новое обновление содержит встроенные антивирусы, поэтому необходимо вовремя обновлять все свои гаджеты. Для операционной системы Android существуют наиболее популярные антивирусные программы, которые можно самостоятельно скачать в Google Play. Это CM Security AntiVirus & AppLock, Kaspersky Internet Security, McAfee Security & Antivirus Free и др».

- **Molnet.ru – Техника безопасности с банковской картой в жизни и в интернете**
  https://www.molnet.ru/mos/ru/finace_investments_credits/o_497996#

«Банки-эмитенты, выпускающие пластиковые карты, стараются максимально повысить их безопасность. Технологии защиты, используемые как при изготовлении, так и для эксплуатации карт, постоянно улучшаются. Это выгодно всем: и банкам и держателям, так как в некоторых проблемных ситуациях ответственность за потерю денег несёт банк. Самое слабое звено в цепочке: клиент-банковская карта-банкомат/терминал в магазине - это, конечно же сам клиент. Всё банковское железо и софт регулярно проходят стресс-тесты по безопасности и регулярно модернизируются, а вот клиенты такие тесты не проходит и каждый раз наступают на одни и те же грабли.

Основные виды мошенничества

Одна из уловок преступников, достаточно часто применяемая для несанкционированного съема денег с банковских карт, – так называемый фишинг. Это способ получения реквизитов карты посредством мошеннического обмана ее владельца. Обычно держателям пластика рассылаются СМС якобы от работников банка, в тексте которых предлагается позвонить по указанному телефону, якобы в банк. При разговоре, под благовидным предлогом, у владельца счета выманиваются данные карты, необходимые для снятия денег или покупок в интернет-магазинах. Распространен также фишинг с использованием рассылок по электронной почте. Владелец счета получает письмо, якобы из банка, где ему предлагается пройти по указанной ссылке. На специально созданном сайте, интерфейс которого, скорее всего, будет очень похож на настоящий банковский, его уже ждет подробная инструкция и окошечки для ввода конфиденциальной информации.

Знайте: Банк никогда не рассылает электронные письма и SMS-сообщения клиентам-держателям карт с просьбой подтвердить номер карты и/или другие идентификационные данные карт, а так же не совершает звонки с этой целью.

Еще одна уловка мошенников – считывание данных с карты с помощью специальных приспособлений, устанавливаемых непосредственно на банкомат. Подобный способ называется скиммингом и используется главным образом на уличных банкоматах в нелюдных или затемненных местах. К устройству может быть прикреплена мини-видеокамера для «подглядывания» за набором пин-кода, а к отверстию для карт крепится специальная накладка для считывания данных – скиммер. Разновидность скимминга – шимминг, при котором в щель устройства внедряется тонкая и гибкая, практически незаметная пользователю электронная плата для фиксации реквизитов карты. На основе полученных данных умельцы изготавливают поддельные карточки и спокойно снимают по ним денежные средства со счета.

Самые распространенные ошибки клиентов согласно мировой статистике

- утеря карты, на которой написан ПИН код;
- владелец карты сообщает третьим лицам данные с карты (включая код CVV);
- владелец карты сам сообщает ПИН код карты;
- добровольное перечисление средств – по схеме стандартного обмана по технологии «Нигерийские письма».

Как видите, самые актуальные способы воровства ваших денег с банковских карт имеют понятную природу обманутых живых людей, а вовсе не технические изыски.

Этих неприятностей можно избежать, если придерживаться золотого правила: никогда, никому и ни под каким предлогом не сообщать никаких данных о банковской карте.

Как бы это ни было печально, но законодательной базы, регламентирующей ответственность банков при осуществлении мошеннических действий с пластиковыми картами, в России пока нет. Все случаи рассматриваются каждым банком в отдельности. Они проводят свое собственное расследование и, как правило, если вы нарушили хоть один пункт договора по использованию пластиковой карты (передали третьим лицам, хранили пин-код в доступном для других месте, сообщали информацию о сроке службы, номере карты или cv1/cv2 коды третьим лицам), то в возврате средств будет отказано. Для того чтобы иметь основания и написать заявление в банк – нужно дождаться подтверждения

прохождения транзакции (около 3-х дней). До этого момента деньги еще фактически находятся на вашем счету, и оснований для обжалования транзакции нет.

Если злоумышленнику удастся получить копию вашей карты без чипа и пин-код, то, скорее всего такие операции не отличить от совершенных вами лично, и тут тоже напрашивается отказ.

Банковская карта

1. Самое главное правило: никогда не носите с собой листочек, на котором написан PIN-код от вашей карты. Никогда не пишите PIN-код на обратной стороне вашей карты, храните его всегда отдельно, лучше всего в вашей памяти. Для усиления защиты меняйте ПИН-код хотя бы раз в полгода. Это можно сделать в любом банкомате. Операция платная, но стоит сущие копейки.
2. Если владельцу карты не безразлична судьба его капитала, то нужно пользоваться только картой с чипом. Ранее такие карты принимали не все банкоматы, но сегодня ситуация изменилась, и если какой-то банк откажет в снятии денег с такой карты, то он будет оштрафован.
3. Если денег на карте много, то обязательно нужно установить суточный лимит на снятие денег. Это позволит сохранить хотя бы часть своих денег. К тому же если деньги срочно понадобятся владельцу, то он может снять ограничения за считанные минуты в онлайн-банкинге.
4. Никогда не передавайте вашу карту третьим лицам. Если вы расплачиваетесь в магазине, всегда держите ее в поле зрения. Родственникам также не следует передавать вашу карту. Не потому, что им нельзя доверять, а потому, что они могут быть невнимательны при использовании карты, и стать жертвами мошенников.
5. Никому никогда не сообщайте данные вашей карты. Мошенники часто рассылают СМС-сообщения о том, что карта заблокирована, и просят перезвонить на такой-то номер. Этого нельзя делать ни в коем случае: мошенники, представившись сотрудниками банка, будут стараться узнать данные вашей карточки. Поэтому следует быть бдительным.
6. Используйте смс-информирование. Это позволит вам сразу же увидеть неизвестные платежи с вашего счета и заблокировать карту, не дожидаясь больших расходов мошенников.
7. Блокируйте карту сразу, как появится подозрительная транзакция, многие банки позволяют производить блокировку/разблокировку карты по телефону.
8. Не храните большие суммы на счете, к которому привязана банковская карта. Многие банки предлагают использовать накопительные счета, движения по которым возможны только по защищенным каналам через интернет. Держите на текущем счету минимальный дневной запас средств и пополняйте его с такого счета через интернет-банкинг по мере необходимости.
9. Имейте несколько каналов блокировки карты на случай кражи. Все знают, что контактные телефоны банка всегда указываются на кредитке, однако не все задумываются, откуда вы их возьмете в случае кражи банковской карточки. Поэтому забейте контакты себе в сотовый вместе с кодовым словом – оно может потребоваться для вашей идентификации при разговоре с сотрудником контактного центра.

10. Старайтесь не вкладывать карту в счет в ресторанах и кафе. В крайнем случае можно попросить официанта сразу принести терминал. Требуйте проводить операции по карте только в Вашем присутствии.

Интернет-покупки

1. Пользователям интернет-банкинга настоятельно советуется по возможности не проводить финансовые операции с компьютеров посторонних лиц, а на своем установить пакет программ безопасности.
2. Пользуйтесь известными интернет-ресурсами. Не указывайте на непроверенных интернет-ресурсах ваши данные банковских карт (номер, имя владельца и срок действия карты). Для совершения покупок, или, как минимум, сайтом с защищенным протоколом обмена данными HTTPS. Наличие данного протокола у сайта узнать довольно легко: это или обозначение замочка перед названием сайта в адресной строке, или буквенное обозначение.
3. Пин-код используется только в банкоматах и подобных устройствах. При интернет-платежах он никогда не применяется (это просто не предусмотрено). Для платежей в интернете необходим так называемый код проверки подлинности CVV2/CVC2, который находится с обратной стороны карты.
4. Лучше, если у магазина есть прямой договор с вашим банком. В таком случае для совершения оплаты вам поступит SMS с подтверждающим перевод кодом.
5. Используйте виртуальную карту – если вы покупаете в непроверенном интернет магазине, то лучшим решением будет расплатиться с помощью виртуальной карты. Все чем вы рискуете – это средствами на ней, так как сразу после оплаты карта становится недействительной. Такую карту можно выпустить онлайн, прямо их админки Интернет банка (не у всех банков это возможно).

Банкомат

1. При снятии денег внимательно отнеситесь к выбору банкомата. Лучше всего воспользоваться аппаратом, установленным прямо в помещении банка, государственном учреждении, торговом комплексе, отеле, аэропорте. Деньги с пластиковой карты лучше снимать исключительно в залах с видеофиксацией. Не пользуйтесь устройствами, требующими пин-код для доступа в кабину с банкоматом.
2. При застревании карты в банкомате или терминале необходимо незамедлительно позвонить в Банк, сообщить о случившемся и заблокировать карту (после этого ни один мошенник не сможет снять ваши деньги. Уходить можно, только когда сотрудник банка подтвердит блокировку карты). Если вы решили ожидать прихода работников банка, не стоит отходить от банкомата.
3. На клавиатуре и картридере не должно быть никаких дополнительных приспособлений. Мошенники могут размещать там накладки, которые запомнят очередность клавиш или считают конфиденциальные данные с электронного носителя.
4. Если вы снимаете крупную сумму, то нет смысла пересчитывать деньги прямо у банкомата – так вы только привлечёте к себе внимание. Даже если банкомат ошибся, что бывает крайне редко (например, программный сбой), то ситуацию сразу не исправить. Совершайте самостоятельно все операции, не просите помощи у посторонних людей, можно обращаться только к сотрудникам банка.

Смартфон

В последнее время практически все российские банки, имеющие развитые мобильные банковские приложения, столкнулись с массовыми случаями краж денег со счетов клиентов. Чаще всего воровство происходит с помощью вируса, внедренного на смартфоне или планшете.

Как же мошенники попадают в ваш смартфон или планшет, даже если он у вас в руках? Самая распространенная лазейка – скачанный вами из интернета зараженный файл с фишинговой программой, которая всего берет под контроль услугу смс-информирования. Действует она в двух направлениях. Во-первых, блокируется функция получения смс о переводах, во-вторых, программа самостоятельно отправляет на номер связи смс-запросы о переводах и списаниях. Таким образом, мошенники с помощью вируса списывают с вашего смартфона деньги, а вы ничего не знаете об этом, так как смс о движении средств по вашим счетам до вас не доходят.

Кража вскрывается в тот момент, когда вы либо хотите снять деньги с карты, либо заходите в онлайн-кабинет вашего банка. Как это ни печально, обвинения в отношении банка в данном случае безосновательны: клиент сам использовал смартфон, сам установил вредоносную программу и не предпринял ничего, чтобы защитить свои средства. Максимум, что вам светит, это заявление о возбуждении уголовного дела в полиции, которое с большой вероятностью будет закрыто.

Если у вас есть смартфон или планшет на платформе Android (или любой другой платформы) с установленным мобильным приложением интернет-банка, вам необходимо:

1. В обязательном порядке установить антивирусное приложение. Даже самый простой и бесплатный поможет вам защититься. Ряд банков облегчает жизнь своих клиентов и встраивает в свое мобильное приложение антивирус, как сделал, к примеру, Сбербанк.
2. Скачивайте только официальные приложения (лучше переходить в магазин с официального сайта бренда) и только с официальных магазинов: Google Play, App Store и Winstore. Регулярно обновляйте их, а также операционку и антивирус.
3. Отключите те сервисы, которыми вы не пользуетесь. К примеру, смс-информирование с возможностью мгновенных платежей. Это и есть самая распространенная лазейка мошенников.
4. Многие банки в своих онлайн-приложениях предлагают методы пассивной защиты. К примеру, они дают возможность клиентам скрывать из видимости счета. В этом случае мошенник, войдя в ваш онлайн-кабинет, не увидит вклад на крупную сумму денег или кредитную карту.
5. Если вы сменили номер телефона, обязательно сообщайте об этом в банк. Самое главное – отключить смс-информирование от этого номера. Ведь спустя какое-то время оператор передаст номер другому человеку.
6. Не оставляйте телефон без присмотра и по возможности блокируйте к нему доступ паролем. Банки также рекомендуют не пользоваться услугами интернет-банков через обозреватель мобильного телефона, если на него приходит СМС-сообщение с подтверждающим одноразовым паролем. В общем, будьте начеку, и соблюдайте основные правила безопасного использования ваших карточек, тогда ваши деньги останутся в целости и сохранности».

- **Ведомости – Как нас обманывают карточные мошенники https://www.vedomosti.ru/finance/articles/2017/09/29/735855-kak-obmanivayut#/galleries/140737493571634/normal/1**

«Ведомости» узнали у банкиров приемы злоумышленников и методы борьбы с ними

«Здравый смысл, логика, бережное отношение к данным карты – вот главные средства, которые помогут обезопасить себя от мошенников», – перечисляет вице-президент холдинга «Русский стандарт» (владеет одноименным банком) Эльдар Бикмаев. Улов злоумышленников в 2016 г. составил 2 коп. с каждого платежа по карте на 1000 руб., говорил бывший первый зампред ЦБ Георгий Лунтовский. И хотя карточный выигрыш мошенников сокращается – в прошлом году они украли на 6% меньше, чем годом ранее, 1,08 млрд руб., – рост безналичных платежей заставляет внимательнее относиться к безопасности карт.

Человеческий фактор

Замначальника Главного управления безопасности и защиты информации ЦБ Артем Сычев называет социальную инженерию «одной из самых больших проблем информбезопасности» и цитирует песню Булата Окуджавы из фильма «Приключения Буратино»: «Пока живут на свете дураки, обманывать нам, стало быть, с руки».

Все опрошенные «Ведомостями» банки согласились, что главная причина кражи денег с карт в том, что клиенты ведутся на обман, с помощью которого мошенники выманивают у них информацию о карте или заставляют проделать определенные манипуляции.

Социальная инженерия работает так, приводит пример Сычев: на телефон жертвы приходит сообщение, что карта заблокирована, а для разблокировки предлагается позвонить по указанному номеру. Жертва перезванивает, а на другом конце провода – злоумышленники, которые представляются сотрудниками банка и вынуждают сообщить информацию о карте или подойти к банкомату якобы для разблокировки. Результат один – жертва сама переводит деньги мошенникам.

Вот история с одного из форумов. Женщина поверила мошенникам, по телефону убедившим ее ввести в банкомате в поле для указания суммы перевода набор цифр и заверившим, что это «код подтверждения». Главное – не звонить по номеру телефона, указанному в смс, говорит Сычев, а пользоваться только номером на обратной стороне карты – уж это точно номер банка, а не мошенников.

В последние пару лет существенно выросло число инцидентов с использованием этого метода, сетует начальник управления мониторинга электронного бизнеса Альфа-банка Владимир Бакулин. С введением технологии 3D Secure (дополнительное подтверждение операции с помощью одноразового пароля, отправленного на телефон. – «Ведомости») технических способов хищения стало меньше, а с использованием социальной инженерии – больше, отмечает вице-президент банка ТКБ Игорь Антонов.

С помощью социальной инженерии мошенники узнают у жертвы реквизиты, достаточные для совершения перевода с карты на карту: номер карты, срок ее действия, CVV-код (с обратной стороны карты), указывает начальник отдела безопасности

банковских карт «ОТП банка» Андрей Леонтьев. Важно помнить, что представители банка никогда – ни по телефону, ни в переписке – не спрашивают полные данные карт, одноразовые пароли, пин-коды, подчеркивает пресс-служба «Тинькофф банка», для консультации им обычно достаточно имени и четырех последних цифр карты.

Другой прием социальной инженерии – рассылка электронных писем с вирусами. Письмо приходит якобы от контрагента, который просит срочно посмотреть новую тарифную сетку, скажем, телекомоператора, приводит пример Сычев. Цель письма одна – заставить открыть прикрепленный документ либо ссылку, которая приведет к загрузке вредоносной программы, объясняет Сычев: «Если вы не будете открывать такие письма или у вас установлен антивирус, это будет гарантировать безопасность ваших денег и вашей информации».

Существует огромное количество подставных сайтов, созданных мошенниками, предостерегает Бикмаев: одно время были сайты «Проверьте, скомпрометирована ли ваша карта», где клиенту предлагалось ввести данные карты, а потом пришедший от банка пароль. Такие сайты созданы для перевода с карты на карту либо перехвата данных, продолжает Бакулин: совершая операцию на подобном сайте, человек вводит данные своей карты, думая, что совершает покупку, однако на самом деле происходит обращение к одному из легальных ресурсов по переводам, где в качестве получателя платежа уже подставлена карта мошенника.

При использовании карты для оплаты в интернете, банкомате или торговой точке банки дают рекомендации, как минимизировать риск кражи денег (см. врез). От того, как вы их исполняете, будет зависеть, станете ли вы добычей злоумышленников, а также сможете ли вернуть деньги, если их все же украдут.

Что делать после кражи

С 2014 г. закон «О национальной платежной системе» обязывает банк вернуть похищенные с карты средства. Но только при соблюдении ряда условий: клиент должен сообщить о краже в течение суток после получения от банка уведомления об операции. Кроме того, компрометация данных карты не должна произойти по вине клиента. Если же банк не уведомил об операции или разрешил ее после сообщения клиента об утрате карты, вся ответственность лежит на банке.

Жалобы, связанные с кражей денег с карт и невозможностью получить возмещение, – третьи по частоте, говорит финансовый омбудсмен Павел Медведев, и вернуть деньги в таком случае удается редко: банки успешно доказывают вину клиента в компрометации карты. Это подтверждает банкир: если клиент сам не передаст информацию о карте или не будет использовать зараженное вирусом устройство, украсть деньги с карты практически невозможно. Статья в законе больше направлена на возврат денег, украденных с карты без чипа, говорит банкир: их мошенники легко подделывают и при их использовании не требуется пин-код – невозможно определить, кто совершает транзакцию. Если же вводится пин-код, банк однозначно определяет, что картой пользуется ее держатель. С 2015 г. банки обязаны выпускать карты только с чипом, других в обращении почти не осталось.

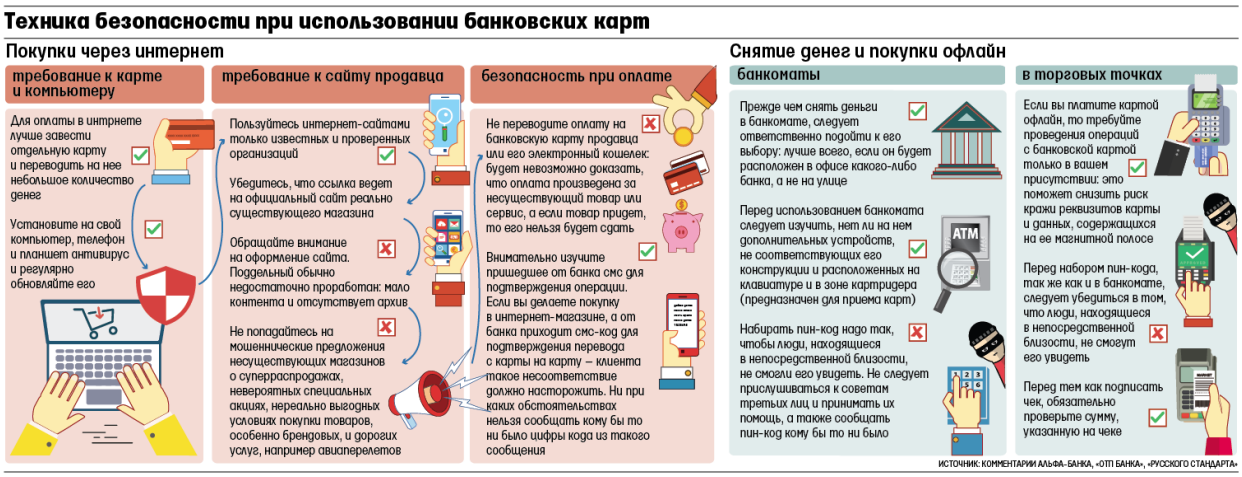
Самая распространенная причина отказа вернуть деньги – несвоевременное уведомление банка о несанкционированном использовании карты или мобильного

телефона, говорит представитель ВТБ. Когда клиент нарушил порядок безопасного хранения и использования карты (например, использовал нелицензированное ПО) и средства похищены из-за заражения устройства вирусом, банк рассматривает подобные ситуации в индивидуальном порядке, указал он. В таких случаях банк рекомендует обратиться в правоохранительные органы.

Медведев не советует обращаться в суды или правоохранительные органы, даже если украли крупную сумму – сотни тысяч рублей: в процессе тяжбы можно лишиться здоровья и оставшихся денег – они уйдут на судебные издержки.

В абсолютном большинстве случаев клиент сам называет свои данные: CVV, пин-код и т. д., что делает невозможным возврат и опротестование операции, а также нельзя доподлинно проверить, что это было мошенничество, а не злонамеренные действия самого клиента, указывает Антонов. За последние три года с изменения закона расходы банка на возмещение клиентам не увеличились, рассказал он.

Россия входит в число благополучных рынков с точки зрения безопасности, говорит специалист по вопросам безопасности Mastercard в России Евгений Балезин: в последние годы ситуация улучшается».



5.2. Правовые вопросы

5.2.1. Федеральный закон N 161-ФЗ "О национальной платежной системе" от 27 июня 2011 г. является основным правовым документом, регулирующим права потребителя при совершении дистанционных платежей, а также обязанности банков и их клиентов по обеспечению безопасности совершаемых дистанционно операций (с особым вниманием к статье 9 "Порядок использования электронных средств платежа" и статье 27 "Обеспечение защиты информации в платежной системе").

Также следует принимать во внимание положения закона "О защите прав потребителей" о праве потребителя на безопасность товара (работы, услуги) (см. например, статью 7 закона).

Ссылки на тексты этих законов см. в Разделе 1 Сборника.

Детально требования Банка России к обеспечению профессиональными участниками защиты информации, средствам и методам обеспечения информационной безопасности раскрыты в Положении Банка России от 9 июня 2012 г. N 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". Положение (в редакции от 07.05.2018 г.) доступно по адресу http://legalacts.ru/doc/polozhenie-o-trebovanijakh-k-obespecheniiu-zashchity-informatsii/.

5.2.2. Статьи, рассматривающие практику и проблемные вопросы правовой защиты прав потребителей.

- **Zakon.ru – Некоторые проблемы, связанные с оспариванием спорных транзакций, совершенных с использованием электронного средства платежа**
  https://zakon.ru/blog/2017/3/14/nekotorye_problemy_svyazannye_s_osparivaniem_spornyh_tranzakcij_sovershennyh_s_ispolzovaniem_elektro

«Кредитные и дебетовые карты набирают в России все большую популярность год от года: люди используют их для оплаты коммунальных платежей, продуктов питания, оказания услуг и многого другого. Появляются различные типы карт (например, кобрендинговые карты), а наличием в условиях пользования картой кэшбека уже вряд ли можно кого-то удивить.

Тем не менее, за кажущейся безоблачностью и простотой скрывается несколько довольно сложных правовых проблем. Остановимся на вопросе об оспаривании транзакций, произведенных с помощью электронного средства платежа без согласия клиента. Стоит отметить, что у данного вопроса существует как интересный гражданско-правовой аспект, так и уголовно-правовой. Рассмотрим подробнее первое.

Данный вопрос регулируется Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе», в частности, ст. 9 данного закона, которая в полном объеме вступила в силу лишь 1 января 2014 года. Необходимо рассмотреть систему оспаривания спорных транзакций, совершенных с использованием электронного средства платежа на настоящий момент.

Так, исходя из положений ст. 9 указанного закона, банк несет ответственность, т.е. обязан выплатить сумму спорной транзакции, лишь в трех случаях: 1) банком не было направлено уведомление клиенту о совершении операции, и при этом операция была совершена без согласия клиента (ч. 13 ст. 9); 2) банк уведомил клиента о совершении операции, и клиент своевременно уведомил банк об утрате электронного средства платежа или его использовании без его согласия (в таком случае банк должен возместить стоимость транзакций, произведенных без согласия клиента до получения от него уведомления только если банк не докажет, что клиент нарушил порядок использования электронного средства платежа, что повлекло совершение операции без согласия клиента) (ч. 15 ст. 9); 3) банк также обязан возместить стоимость транзакций, произведенных банком после получения уведомления об утрате электронного средства платежа или его использования в отсутствие согласия клиента (ч. 12 ст. 9).

Интересным вопросом представляется определение согласия клиента на совершение той или иной транзакции с использованием электронного средства платежа. Не останавливаясь слишком подробно на этом вопросе, скажем лишь, что по общему правилу банк может предполагать наличие согласие клиента на совершение операции в случае, если при использовании электронного средства платежа был корректно введен ПИН-код, либо

при использовании карты были корректно названы ее реквизиты, известные лишь владельцу (в частности, коды CVV/CV2 и пр.).

Ключевая проблема, связанная с рассматриваемой проблемой, заключается в том, что на практике ч. 15 ст. 9 ФЗ «О национальной платежной системе», подразумевающая обязанность банка возместить стоимость спорных транзакций, произведенных до поступления уведомления об утрате карты или ее использовании без согласия клиента, не работает. Это связано с тем, что банки при выпуске карт обязательно включают в правила пользования электронным средством платежа подобные пункты: «Риски, связанные с проведением третьими лицами операций в случае Утраты Банковской карты/Компрометации Банковской карты, в том числе по операциям, проведенным по банковским картам, неправомерно созданным третьими лицами с использованием реквизитов Банковской карты при Утрате Банковской карты/Компрометации Банковской карты, несет Клиент до момента информирования Клиентом Банка с целью блокировки Банковской карты» и аналогичные.

Экономический интерес банков очевиден: ни одна кредитная организация не заинтересована в том, чтобы принять на себя риски, связанные с пренебрежительным отношением клиентов к конфиденциальности реквизитов карты, безопасности ее хранения, хранения ПИН-кода и прочего. Потребители, как следствие, оказываются в ситуации, когда в случае утраты карты, счет идет на минуты. К примеру, в деле, описанном в Апелляционном определении Московского городского суда от 08.10.2014 по делу № 33-33043, Истец (владелец карты) обнаружил, что в период с 07:06 до 09:14 утра были совершены несколько транзакций без его согласия, и уже в 10:58 он обратился с соответствующим уведомлением к Ответчику (банку). В дальнейшем потребовал возврата стоимости спорных транзакций. В итоге в удовлетворении требования было отказано на том основании, что злоумышленник ввел секретные коды CVV/CV2, что позволило банку предполагать согласие клиента, в то время как риски компрометации карты третьими лицами, согласно правилам данного банка, лежит на владельце карты.

При этом императивное исключение возможности включать указанные ранее пункты в правила пользования электронным средством платежа выглядят неоправданными, поскольку при таком регулировании выпуск банковских карт в обращение резко сократится, или условия их выпуска приобретут очевидно неблагоприятный для потребителей характер. Возникнет ситуация, когда от такого регулирования правил использования электронных средств платежа, направленного на защиту прав и интересов потребителей, пострадают сами же потребители (т.н. эффект переноса экономического бремени на контрагентов, «passing along»).

Более того, стоит отметить, что такое регулирование также представляется слабо реализуемым ввиду наличия некоторого количества недобросовестных лиц, которые намеренно могут злоупотреблять своими правами, заявляя о несогласии с проведенными транзакциями (хотя они проводились ими же), чтобы взыскать с банка денежные средства (т.н. дружеский фрод, «friendly fraud»). Наличие подобных мошенников в условиях императивного регулирования правил пользования электронными средствами платежа усугубит ситуацию ввиду такого явления, как ухудшающий отбор (adverse selection), подразумевающий в контексте описываемой проблемы, что за счет наличия рисков столкнуться с мошенниками, банк будет ухудшать условия для потребителей, дабы этот

риск компенсировать, что в конечном счете приведет к тому, что добросовестные потребители откажутся от вступления в договорные отношения с банком ввиду явно несправедливых и невыгодных условий, в то время как недобросовестные потребители продолжат использовать обозначенную схему. Таким образом, в конечном счете доля недобросовестных владельцев карт будет неминуемо расти.

Представляется, что в решении описанной проблемы может помочь установления на законодательном уровне обязательности предложения банками, осуществляющими выпуск карт, клиенту заключения договора страхования банковской карты. На сегодняшний день многие крупные банки предлагают подобные услуги (страхование банковской карты, например, возможно в Сбербанке России, Райффайзен Банке и некоторых других). Представляется, что в случае, если банки в обязательном порядке будут предлагать своим клиентам застраховать риски, связанные с утратой карты, во-первых, увеличится число застрахованных карт, что в итоге приведет к снижению случаев безвозвратной утраты денежных средств, во-вторых, в случае, если клиент отказывается от заключения договора страхования, он на когнитивном уровне осознает, что берет риски, связанные с утратой и компрометацией карты на себя (в противовес сложившейся сегодня ситуации, когда клиенты полагают, что именно банки виноваты в том, что закрепили такие несправедливые правила пользования, которые большинство потребителей внимательно не изучают). В то же время необходимо понимать, что у такого подхода есть недостатки: так, не все мелкие и средние банки, осуществляющие выпуск карты, способны на сегодняшний день предложить услуги по страхованию. В случае же кооперации со страховыми компаниями, неизбежно сложится ситуация, в которой спрос на услуги по страхованию банковских карт искусственно увеличивается, что в свою очередь приводит или к увеличению стоимости (центрального условия договора), или к ухудшению так называемых «периферийных» условий договора. Тем не менее, представляется, что в сложившейся ситуации, такой подход является оптимальным.

Стоит отметить, что императивное установление обязательного страхования банковских карт представляется неоптимальным путем урегулирования проблемы, поскольку приведет к многократному увеличению транзакционных издержек, разрушению (или во всяком случае нанесению существенного урона) бизнес-стратегий, основанных на бесплатной выдаче и доставке банковских карт (как это, например, реализуется в банке Тинькофф), а также иным проблемам. Кроме того, считаем, что такая мера явилась бы мерой излишнего патернализма со стороны государства, который в условиях рыночной экономики должен ограничиваться.

Таким образом, исходя из сказанного, считаем, что ст. 9 Федерального закона «О национальной платежной системе» необходимо дополнить пунктом об обязательности предложения банком клиенту услуг по страхованию электронного средства платежа на случай его утраты или компрометации».

- **Zakon.ru – О положительной практике в делах о взыскании с банка незаконно списанных денежных средств**
  https://zakon.ru/blog/2016/9/23/o_polozhitelnoj_praktike_v_delah_o_vzyskanii_s_banka_nezakonno_spisannyh_denezhnyh_sredstv

«И снова вести с банк-онлайновских полей.

Говоря о сложностях возврата незаконно списанных с банковских счетов (включая открытые в Сбербанке) денежных средств, рассмотрим также положительную для вкладчиков и держателей карт практику.

Как говорилось ранее, заявляя об отсутствии в действиях банка нарушений, его представители, как правило, аргументируют свою позицию тем, что, в зависимости от ситуации:

- по данным системы клиент банка дал поручение и согласие на перевод или вывод средств посредством ввода ему одному известного идентификатора, постоянного и одноразовых паролей;

- на устройстве пользователя может быть установлено вредоносное ПО, с помощью которого злоумышленники получили доступ к счету;

- владелец счета сам сообщил данные доступа третьим лицам.

Удовлетворяя требования пострадавших, суды берут за основу не содержание банковских договоров и положений банка, а федеральное законодательство.

В частности, ч. 15 ст. 9 ФЗ "О национальной платежной системе" обязывает вернуть перечисленные без согласия владельца счета денежные средства, если банк не докажет, что клиент нарушил порядок использования электронного средства платежа, что повлекло совершение операции без согласия клиента - физического лица.

Бремя доказывания обстоятельств, освобождающих от ответственности, ложится на банковскую организацию также в соответствии с ч. 4 ст. 13 Закона РФ "О защите прав потребителей". Соответствующие разъяснения даны и в постановлении Пленума ВС РФ от 28.06.2012 № 17.

О том, какие факты будут являться доказательством нарушения клиентом порядка использования электронного средства платежа, ни законодатель, ни суд не говорят. Но соблюдение условий договора о применении должной степени осмотрительности и заботливости в отношении самой карты и данных доступа, а также порядка и срока уведомления банка о нарушении и блокировке карты должны быть соблюдены.

При этом, достаточно весомым доводом в пользу позиции истца будет являться подтверждение факта обращения в правоохранительные органы, возбуждение уголовного дела и признание заявителя потерпевшим.

В одном из случаев в рамках досудебных мероприятий было установлено также, что в тот период времени, когда проводились операции по переводу денежных средств, пострадавшая выход в интернет не осуществляла, а IP-адрес, с которого поступил запрос и подтверждение на перевод находится в другом регионе. Более того, правоохранители установили, что на счет получателя платежа в течение суток поступила достаточно крупная сумма денег из разных регионов страны (апелляционное определение Суда Еврейской автономной области от 01.07.2016 по делу № 33-423/2016).

Основной аргумент банка о возможном заражении оборудования клиента вирусом не учитывается судами, поскольку ч. 1 ст. 4 Закона о защите прав потребителей возлагает на исполнителя обязанность по оказанию услуги, соответствующей условиям договора. А, согласно ч. 2 ст. 7 указанного закона, банк должен обеспечить безопасность услуги, в т.ч.

для имущества потребителя. Другими словами, предлагаемое владельцам счетов мобильное приложение должно быть защищено настолько, насколько это необходимо для его качественной работы, в т.ч. для предотвращения заражения вирусами (апелляционное определение Артемовского городского суда Приморского края от 23.06.2016 по делу № 11-40/2016)».

Интересен анализ судебной практики по спорам в результате хищений через каналы дистанционного банковского обслуживания (ДБО), подготовленный экспертами консультационной фирмы RTM TECHNOLOGIES. Доклад можно скачать по ссылке https://rtmtech.ru/issledovaniya/.

- **Гарант – ВС РФ: риск неправомерного списания со счета денежных средств посредством дистанционных сервисов несет банк http://www.garant.ru/article/1091934/**

«По общему правилу списание денежных средств со счета осуществляется банком на основании распоряжения клиента (п. 1 ст. 854 Гражданского кодекса). Означает ли это, что именно на банк возложены риски, связанные с выдачей денежных средств лицу, не уполномоченному на их получение? Суды первой и апелляционной инстанций не смогли прийти к единому мнению, поэтому Верховному Суду Российской Федерации пришлось обозначить свою позицию.

Суть спора

В марте 2012 года гражданка Е. (далее – истец) получила выпущенную банком «С» (далее – ответчик) кредитную карту. Услуга «Мобильный банк» была подключена на номер ее супруга. Начиная с мая 2013 года, после того, как задолженность по кредиту была погашена, Е. банковской картой не пользовалась. Между тем в декабре того же года оператор связи «Б» в одностороннем порядке прекратил обслуживание абонентского номера, закрепленного за супругом истца, в связи с его неиспользованием более 180 дней и затем предоставил его другому абоненту. Как следует из материалов дела, услуга «Мобильный банк» не была отключена.

Спустя еще полгода банк обратился к истцу с требованием погасить задолженность по принадлежащей ей кредитной карте в размере 176 тыс. руб. Из присланной истцу телеграммы следовало, что денежные средства были обналичены в период с 29 апреля по 7 мая 2014 года посредством услуги «Мобильный банк» с номера телефона оператора "Б". Учитывая, что операции по карте «Е» не производила, она обратилась в банк с заявлением о списании неправомерно начисленной, по ее мнению, задолженности. Однако ни банк «С», ни сотовый оператор «Б», к которому она также направила обращение с целью урегулирования возникшей ситуации, оставили их без удовлетворения. Тогда по заявлению «Е» было возбуждено уголовное дело, по которому она была признана потерпевшей. Затем Е. обратилась в суд с иском о признании обязательств по кредитному договору исполненными в полном объеме.

Суд первой инстанции требования истца удовлетворил (решение Пушкинского городского суда Московской области от 3 декабря 2015 г. по делу № 2-5374/2015). При этом судья в своем решении отметил, что долг по кредитной карте возник вследствие действий третьих лиц и в отсутствие воли истца, в связи с чем обязанность погасить задолженность у гражданки Е. отсутствует.

Однако суд апелляционной инстанции, куда обжаловал решение суда первой инстанции ответчик, это решение отменил. При этом в новом решении по делу суд указал на то, что истец, в нарушение установленных банком правил выпуска и обслуживания кредитной карты, не сообщила сотрудникам банка о прекращении использования абонентского номера, к которому была подключена услуга дистанционного обслуживания. Суд также подчеркнул, что истец не предприняла необходимых для отключения этой услуги действий.

Позиция ВС РФ

КРАТКО

Реквизиты решения: Определение СК по гражданским делам ВС РФ от 10 января 2017 г. № 4-КГ16-66.

Требования заявителя: Отменить апелляционное определение, согласно которому суд отказался признать обязательства истца перед банком исполненными ввиду того, что она не уведомила его сотрудников о прекращении использования абонентского номера, к которому была подключена услуга "Мобильный банк".

Суд решил: Апелляционное определение отменить, дело направить на новое рассмотрение в суд апелляционной инстанции.

Не согласившись с апелляционным определением, истец обратилась с жалобой в ВС РФ о его отмене. Рассмотрев кассационную жалобу, ВС РФ пришел к выводу о том, что основания для ее удовлетворения все же имеются (Определение СК по гражданским делам Верховного Суда РФ от 10 января 2017 г. № 4-КГ16-66).

Так, члены Судебной коллегии по гражданским делам ВС РФ отметили, что согласно нормам гражданского законодательства обязательство заемщика заключается в возврате полученных им по кредитному договору денежных сумм (п. 1 ст. 810, п. 1 ст. 819 ГК РФ). Более того, ни волеизъявления истца на получение кредита, ни ее распоряжений о совершении операций по счету в период с 29 апреля по 7 мая 2014 года не было. Также у нее отсутствовала и техническая возможность для этого. При таких обстоятельствах вывод суда апелляционной инстанции о наличии у гражданки Е. как заемщика долга, вытекающего из кредитного договора, противоречит нормам ГК РФ, указали судьи.

Одновременно ВС РФ пришел к выводу, что вопрос о причинении банку убытков вследствие неуведомления о прекращении использования номера телефона и его передаче третьему лицу к предмету рассмотрения дела не относится.

ВС РФ также добавил, что риск ответственности за последствия исполнения поручений, выданных неуполномоченными лицами, несет именно банк. Так, списание денежных средств со счета осуществляется банком на основании распоряжения клиента (п. 1 ст. 854 ГК РФ). Также из обстоятельств дела следует, что для подтверждения распоряжения о переводе денежных средств на указанный в договоре номер клиента банк направляет неперсонифицированные пароли. Как пояснили суду представители банка, это необходимо для предотвращения исполнения ошибочных и случайных распоряжений, однако из этого не следует, что таким образом идентифицируется владелец счета либо его доверенное лицо, владеющее соответствующим кодом или паролем. При этом операция ввода одноразового пароля доступна любому лицу, подчеркнули они.

Поэтому, ВС РФ пришел к выводу, что положения норм материального права применительно к обстоятельствам дела, не были учтены судом апелляционной инстанции. А бремя несения негативных последствий, вызванных выдачей банком денежных средств не уполномоченному на их получение лицу, на истца возложено необоснованно.

В результате ВС РФ определил отменить обжалуемое определение, и дело было направлено на новое рассмотрение.

Позиция юристов

Очевидно, что с развитием сервисов дистанционного обслуживания, услуги которых предоставляются не только банками, но и различными электронными платежными системами, а также операторами мобильной связи, число рассматриваемых судами дел, подобных этому, будет только расти (Определение СК по гражданским делам Верховного Суда РФ от 8 декабря 2015 г. № 5-КГ15-164, Постановление Московского городского суда от 28 июля 2016 г. № 10-10379/16 и другие). Причем, практика показывает, что гарантированной защитой от действий злоумышленников не могут похвастать финансовые организации, работающая через Интернет. Однако, отмечая обоснованность и закономерность вывода ВС РФ, эксперты подчеркивают, что несмотря на знаковость этого события, говорить о том, что все без исключения суды в аналогичных обстоятельствах теперь будут принимать решения в пользу клиентов банков пока рано. «Позицию суда необходимо закрепить в законодательстве», – полагает адвокат Сергей Воронин.

Специалисты также настаивают, что банки должны уделять больше внимания обеспечению безопасности своих клиентов. Так, директор ООО «БРУКС кредитный консультант» Алексей Пермяков считает, что авторизация клиентов в приложениях мобильного банкинга не должна происходить только лишь по номеру телефона. Для защиты денежных средств клиента, в том числе кредитных, банк обязан запрашивать и другие персональные данные, которые не могут быть известны третьему лицу, подчеркивает он.

Аналогичной позиции придерживается и Елена Орлова, генеральный директор сервиса электронных платежей Platron. «В последнее время действительно участились ситуации, когда операции по банковской карте, проведенные через мобильный банк, оспариваются клиентами и основными их доводом является незаконность списания денег, так как денежные средства снимаются помимо их воли. Несмотря на огромные вложения, которые делают банки на постоянные обновления и повышения эффективности системы безопасности, – сбои случаются. Так, банк действует по стандартной процедуре: при поступлении распоряжения от клиента (введение паролей, подтверждение оплаты и т. д.) происходит идентификация владельца карты и транзакция либо успешно проводится, либо происходит отказ в переводе. Но и такая система удостоверения личности клиента неидеальна. Поэтому отнесение ответственности за несанкционированное списание денег именно на банк закономерно. Помимо действующих мер защиты от мошенников, полагаю, банкам стоит задуматься о том, чтобы повысить безопасность оплаты через мобильных операторов и усовершенствовать их стандарты безопасности,» – отметила она.

Павел Дашевский, генеральный директор DOLGI.ru:

«Как не стать жертвой мошеннических операций по банковским картам? Во-первых, если есть возможность оплатить покупку наложенным платежом или курьеру – лучше

выбрать именно такой способ оплаты. А если покупки в Интернете являются неотъемлемой частью вашей жизни, лучше завести отдельную карту, возможно даже ее виртуальный аналог, чтобы использовать ее только для онлайн-покупок.

Во-вторых, широко известное правило: никому и никогда, ни при каких условиях нельзя сообщать свой PIN, а также трехзначный код CVV2/CVC2 на оборотной стороне банковской карты. Кроме того, не стоит сохранять идентификационную информацию о банковских картах в своих смартфонах для более быстрой оплаты – вредоносные вирусы могут с легкостью заполучить и использовать персональную информацию. А если вы решили погасить штрафы или другие задолженности на крупные суммы, стоит убедиться, что ваш банк, собственностью которого является платежная карта, использует технологии повышенной кибербезопасности, например, 3-D Secure/Secure code.

В-третьих, если ваш гаджет подключен к общественной беспроводной сети – ни в коем случае не стоит совершать каких-либо транзакций через смартфон, поскольку публичные сети – место обитания кибермошенников. Не стоит также хранить на банковских картах крупные суммы денег, а также оплачивать с помощью "пластика" крупные покупки: такие операции, во избежание недоразумений, стоит совершать с помощью банковских счетов или ячеек. Но если на ваш смартфон приходят странные SMS, касающиеся банковских операций по вашей карте, стоит незамедлительно обратиться в банк – нередки случаи, когда «привязанные» номера телефонов к картам служат легким способом доступа к вашим сбережениям посредством онлайн-банкинга. В заключение, стоит отметить, что не стоит скупиться на покупку антивирусных программ для ваших гаджетов, а также на приобретение страховки для своих банковских карт. Эти долгосрочные вложения в перспективе могут существенно облегчить процедуры возврата денежных средств при столкновении с кибермошенниками».

5.3. Судебные решения по вопросам кредитных обязательств жертв интернет-мошенников

Обратите внимание, что практика судов неоднозначна – при предъявлении потребителем суду убедительных доказательств, суд принимает сторону потребителя. Однако бремя доказывания возлагается на потребителя.

Из форумов:

«Позвонили мошенники «Н» организации в которой я ранее вкладывала деньги, предложили вернуть мне мои вложения, попросили номер карты куда можно сделать перевод. Я сообщила номер карты банка Тинькофф. Они зашли в личный кабинет, там два счета, дебетовый и кредитный. С кредитки перевели на дебетовую и уже с нее вывели все деньги. Я сразу позвонила в банк сообщила что я ни каких операций не производила. Банк заблокировал кабинет и счета, оператор записал номер с которого звонили, время и .т.д. Через 2 дня мне пришло смс от банка в отказе в моем обращении об отказе операции. Оперативно пересчитали кредитную карту и выдали мне график платежей по кредиту, со всеми процентами, переводами и снятиями наличных денег. Сумма получилась 127000 руб.
В этот же день после общения с банком я обратилась в полицию с заявлением о мошенничестве.
Сделала запрос в банк о предоставлении мне выписки по счетам и адрес где открыты счета.
Пока шел процесс полицейской проверки написала заявление в банк с просьбой

приостановить действие кредитного договора на время расследования, в доказательство приложила копии талонов КУСП.

Банк мне отказал с такой формулировкой.
«ххххх ххххх, здравствуйте!
Относительно совершенных операций по картам, информация ранее Вам была предоставлена.

Отсрочек платежа банк не предоставляет, оплату в любом случае необходимо производить.

Сумма к оплате ххххх руб. Дата платежа хх.хх.хххх г.
Согласно п. 5.10. договора, Вы обязаны ежемесячно оплачивать минимальный платеж в размере и в срок, указанные в выписке. При неоплате минимального платежа по счету применяются штрафные начисления.

Отдел финансовых консультаций «Тинькофф Банк» (АО)».

Сейчас заявление из полиции передали в прокуратуру, где в течении 30 дней как мне сообщили будет решение.

Платеж в банк по кредиту наступит раньше.

Вопрос:
1 Как приостановить действие кредитного договора на время расследования?
2 Как я могу получить от банка более подробную выписку о совершенных операция. (на какой счет выводились деньги, в какой банк или в каком банкомате были сняты?)
3 Действует ли кредитный договор в данном случае на который операется банк с требованием выплаты?

Lenda885 пишет:

1. Как приостановить действие кредитного договора на время расследования?
2. Как я могу получить от банка более подробную выписку о совершенных операция. (на какой счет выводились деньги, в какой банк или в каком банкомате были сняты?)
3. Действует ли кредитный договор в данном случае на который операется банк с требованием выплаты?

1. Никак.
2. Кто сказал,что на счет,а не по номеру карты? Сообщать его вам банк не обязан.
3. Да. Встречный вопрос: как только по номеру карты мошенники зашли в ЛК? Без пароля, что ли?»

«Lenda885 пишет:
есть ли шанс что банк законно не сможет предъявить притенении по кредиту?

Уважаемая, использование личного кабинета в интернет- банке приравнивается к тому, что вы лично потратили эти средства. Случаев, описанных тут вами хоть отбавляй, и еще никто обратного в суде не доказал».

5.3.1. Решения по искам о признании незаконным начисления задолженности по кредиту

Решение № 2-1244/2018 2-1244/2018 ~ М-825/2018 М-825/2018 от 29 мая 2018 г. по делу № 2-1244/2018

Орехово-Зуевский городской суд (Московская область) – Гражданские и административные

№ 2-1244/2018

РЕШЕНИЕ

ИМЕНЕМ РОССИЙСКОЙ ФЕДЕРАЦИИ
29 мая 2018 года г. Орехово-Зуево

Орехово-Зуевский городской суд Московской области в составе председательствующего судьи Щипанова И.Н.,
при секретаре Ивченко Н.П.,
с участием истца Гаврилова О.М. и его представителя по доверенности Гуркиной Т.А., представителя ответчика ПАО «Сбербанк России» по доверенности Кубряковой О.Г., третьего лица, не заявляющего самостоятельные требования на предмет спора, ФИО рассмотрев в открытом судебном заседании гражданское дело по исковому заявлению Гаврилова О.М. к ПАО «Сбербанк России» о защите прав потребителя,

УСТАНОВИЛ:

Гаврилов О.М. обратился в суд с иском к ответчику ПАО «Сбербанк России» с требованиями о расторжении договора банковского счета**кредитной карты** №, признании незаконным начисления задолженности по **кредитной карте** за период с ДД.ММ.ГГГГ по ДД.ММ.ГГГГ в размере 44265 руб. 55 коп., взыскании компенсации морального вреда 30000 руб. и судебных расходов.

В обоснование указано, что ДД.ММ.ГГГГ получил **кредитную карту** Visa Gold **с кредитным** лимитом 50000 руб. сроком на 3 года, с бесплатным годовым обслуживанием, стоимостью **кредита** 19,2 % годовых. Указанной **картой** он не пользовался, хранил дома. В ДД.ММ.ГГГГ г. он узнал, что с его зарплатной **карты** списали денежные **средства** в счет погашения задолженности по **кредитному**договору. Данная задолженность образовалась в период с ДД.ММ.ГГГГ по ДД.ММ.ГГГГ, когда **с кредитной** банковской **карты** №, оформленной на его имя, списано 48000 руб. Денежные **средства** были списаны путем их перевода на различные телефонные номера. При заполнении заявления на получение указанной выше **кредитной карты** он не указывал номер телефона для использования услуги «Мобильный банк», а в качестве телефона для связи указал домашний телефон и сотовый телефон своей матери. Однако никакой информации и паролей на телефон в период списания денежных **средств** не поступало. По факту кражи указанных выше денежных**средств** по его заявлению возбуждено уголовное дело №, предварительное следствие по которому приостановлено в связи с не установлением лица, подлежащего привлечению в качестве обвиняемого. На его обращения к ответчику с просьбой прекратить договорные отношения и закрыть счет на

обслуживание **кредитной карты** он получил отказ. Банк обратился к мировой судье с заявлением о выдаче судебного приказа о взыскании с него задолженности по указанной **кредитной карте** и приказ был выдан. Узнав об этом, он обратился к мировой судье с заявлением об отмене судебного приказа, который был отменен. Считает, что ответчик нарушил положения дей1ствующего законодательства и его права, как потребителя. Он не был своевременно информирован о совершении каждой операции по списанию денежных **средств**, вход в систему осуществлялись не с его мобильного устройства, одноразовые пароли ему не направлялись. Фактически банк осуществлял списание денежных **средств** по распоряжением неуполномоченного на это лица.
В судебном заседании истец и его представитель поддержали заявленные требования по основаниям, указанным в исковом заявлении. При этом сторона истца настаивает на том, что Гаврилов О.М. при оформлении указанного **кредитного** договора не давал в установленной форме своего согласия на подключение к услуге «Мобильный банк», **кредитными средствами** не пользовался, действовал добросовестно. Сообщений о списании денежных **средств** на мобильный телефон, указанный в заявлении, не поступали. Также обращает внимание на то, что банком не была обеспечена должная безопасность операций клиента с использованием электронного **средства** платежа, а вместо этого клиентам банка предлагается страховать свои вклады. В настоящее время у мирового судьи в производстве имеется гражданское дело по иску ПАО Сбербанк России к нему о взыскании указанной выше **кредитной** задолженности, которое приостановлено до разрешения настоящего спора. Обращение при изложенных обстоятельствах Банка к нему с таким иском нарушает его права потребителя, т.к. каких-либо злоупотреблений правом или противоправных действий со стороны истца не было.
Доводы истца в судебном заседании поддержала его мать – ФИО, привлеченная к участию в деле в качестве третьего лица, не заявляющего самостоятельные требования на предмет спора.

Представитель ответчика ПАО «Сбербанк России», представляющая также интересы третьего лица, указанного в иске – Среднерусского банка ПАО Сбербанк (<адрес>) в судебном заседании исковые требования не признала. При этом заявила ходатайства о применении срока исковой давности к указанным правоотношениям, т.к. о том, что его право нарушено истец узнал еще <адрес>., что следует из его искового заявления.
По существу заявленных исковых требований сторона ответчика пояснила, что между сторонами заключен смешанный договор, содержащий элементы договора банковского счета и **кредитного** договора. То есть закрытие счета **карты** возможно лишь при условии погашения овердрафта, что соответствует положениям ст. 421 Гражданского кодекса Российской Федерации, регулирующим отношения по смешанному договору. Банк открыл счет на имя истца, то есть совершил действия (акцепт) по принятию оферты клиента, изложенных в заявлении от ДД.ММ.ГГГГ на получение **кредитной карты** на условиях и тарифах по **картам** Сбербанка России. Данный договор по существу является договором присоединения, основные положения которого в одностороннем порядке сформулированы Сбербанком России в Условиях выпуска и обслуживания **кредитной карты** ОАО «Сбербанк России», которые находятся в свободном доступе. Со стороны Банка не было нарушений указанных Условий. Подписав заявление на получение **кредитной карты,** Гаврилов О.М. согласился с этими Условиями и обязался их выполнять, что следует из п. 4 его заявления. В соответствие с п. 1.4 Условий, Банк осуществляет выдачу **карты** при

условии подключения к **карте** услуги «Мобильный банк». К указанной **карте** была подключена услуга «Мобильный банк» к номеру, указанному истцом в заявлении. Получив соответствующие распоряжения клиента посредством **средства** мобильной связи, Банк провел соответствующие операции с уведомлением клиента посредством СМС-сообщений, направленных на указанны истцом номер телефона, которые были доставлены на этот номер. В связи **с** образовавшейся **кредитной** задолженностью, истцу направлено уведомление о необходимости ее погашения, а потом банк обратился в суд. Полагает, что законных оснований для удовлетворения заявленных требований не имеется, поскольку факты **хищения** у истца с его счета банковской **карты кредитных средств** , возбуждения уголовного дела и признания его по этому делу потерпевшим не влияют на право банка требовать от истца погашения образовавшейся задолженности по **кредитной карте** . В возражение против применения к правоотношениям срока исковой давности, сторона истца пояснила, что его права потребителя были нарушены действиями ответчика, подавшего в ДД.ММ.ГГГГ иск о взыскании указанных выше денежных **средств** с истца. До этого он вел внесудебную переписку, как потребитель банковской услуги и надеялся урегулировать вопрос во внесудебном порядке.

Исследвав доводы иска, выслушав участников процесса, представленные письменные пояснения стороны истца и возражения ответчика, изучив письменные материалы дела, оценив представленные доказательства по правилам ст. 67 ГПК РФ, суд пришел к следующему.

Рассматривая ходатайство представителя ПАО «Сбербанк России» о применении к правоотношениям срока исковой давности, суд пришел к выводу об отсутствии для этого законных оснований.

Частью 1 ст. 181 ГК РФ установлено, что срок исковой давности по требованию о применении последствий недействительности ничтожной сделки составляет три года. Течение срока исковой давности по указанному требованию начинается со дня, когда началось исполнение этой сделки.

Статьей 200 ГК РФ установлено, что течение срока исковой давности начинается со дня, когда лицо узнало или должно было узнать о нарушении своего права. В соответствии со ст. 199 ГК РФ, исковая давность применяется судом только по заявлению стороны в споре, сделанному до вынесения судом решения. Истечение срока исковой давности, о применении которой заявлено стороной в споре, является основанием к вынесению судом решения об отказе в иске.

Указанное исковое заявление подано в связи с нарушением, по-мнению истца, действиями ответчика, предъявившего к нему иск о взыскании задолженности по **кредитному** договору, его прав потребителя. То есть в данном случае срок начинает течь не со дня, когда истец узнал о незаконном списании с его счета денежных **средств** , а с момента, когда он узнал о предъявлении к нему ответчиком иска о взыскании указанных денежных **средств** . При таких обстоятельствах срок исковой давности истцом не пропущен.

Однако, оснований для удовлетворения исковых требований Гаврилова О.М. по основаниям, указанным в иске, не имеется.

Как установлено судом пояснениями участников процесса и представленными ими документами, ДД.ММ.ГГГГ истец обратился с заявлением к ответчику на получение международной **кредитной** банковской **карты** Visa Gold **с кредитным** лимитом 50000 руб. сроком ДД.ММ.ГГГГ, стоимостью **кредита** 17,9 % годовых, в связи с чем банк на имя

истца открыл счет №, т.е. совершил действия (акцепт) по принятию оферты клиента, изложенной в заявлении от ДД.ММ.ГГГГ на получение **кредитной карты** на условиях и тарифах по **картам**Сбербанка России. **Кредитная карта** № истцом была получена. Данный договор по существу является договором присоединения, основные положения которого в одностороннем порядке сформулированы Сбербанком России в Условиях выпуска и обслуживания **кредитной карты** ОАО «Сбербанк России», которые находятся в свободном доступе.

Исходя из пункта 2.4. Условий использования банковских **карт** ПАО Сбербанк, являющихся приложением № 3 к Альбому, **карта** может быть использована держателем для оплаты товаров и услуг, получения/взноса наличных денежных **средств** в **кредитных** организациях и через банкомат с модулем приема наличных и информационно-платежный терминал, а также для совершения иных операций.

Согласно ст. 845 Гражданского кодекса Российской Федерации такой договор является договором банковского счета.

Другим элементом договора о выдаче и использовании **кредитной** банковской **карты** является **кредитный** договор (соглашение о**кредитовании** банковского счета держателя, к которому в соответствии со ст. 850 Гражданского кодекса применяются правила о**кредитном** договоре). Таким образом, между сторонами заключен смешанный договор, содержащий элементы договора банковского счета и **кредитного**договора.

Согласно п. 3 ст. 421 Гражданского кодекса Российской Федерации стороны могут заключить договор, в котором содержатся элементы различных договоров, предусмотренных законом или иными правовыми актами (смешанный договор). К отношениям сторон по смешанному договору применяются в соответствующих частях правила о договорах, элементы которых содержатся в смешанном договоре, если иное не вытекает из соглашения сторон или существа смешанного договора. Таким образом, смешанный договор регулируется правилами о договорах, входящих в его состав. Однако если указанные правила будут противоречить существу смешанного договора или соглашению сторон по такому договору, то они применяться не будут. В соответствии с п. 1 ст. 819 Гражданского кодекса Российской Федерации по **кредитному** договору банк или иная **кредитная** организация (кредитор) обязуются предоставить денежные **средства** (**кредит**) заемщику в размере и на условиях, предусмотренных договором, а заемщик обязуется возвратить полученную денежную сумму и уплатить проценты на нее.

При этом, исходя из существа смешанного договора, обязанность возвратить полученные в **кредит** денежные **средства** взаимоувязана с проведением операций по банковскому счету, включая его закрытие.

Как предусмотрено п. 4.12 Условий использования банковских **карт** ОАО «Сбербанк России», являющихся приложением № 1 к Условиям банковского обслуживания физических лиц ОАО «Сбербанк России», закрытие счета **карты** и возврат остатка денежных **средств со** счета**карты** производится по заявлению клиента при условии погашения овердрафта, отсутствия иной задолженности и завершения мероприятий по урегулированию спорных транзакций по истечении 45 календарных дней с даты подачи заявления о закрытии **карты** , выпущенной к счету **карты**.

Таким образом, соглашением сторон предусмотрено, что закрытие счета **карты** возможно при условии погашения овердрафта, что соответствует положениям

ст. 421 Гражданского кодекса Российской Федерации, регулирующим отношения по смешанному договору.
При таких обстоятельствах суд не вправе применить правила п. 1 ст. 859 Гражданского кодекса Российской Федерации о возможности расторжения договора банковского счета в любое время по заявлению клиента, то есть самих по себе правил о банковском счете без учета правил о **кредитном** договоре, поскольку это противоречит существу смешанного договора о выдаче и использовании **кредитной**банковской **карты** , что согласно п. 3 ст. 421 Гражданского кодекса Российской Федерации недопустимо, поэтому оснований для удовлетворения заявленных требований в этой части не имеется.
Рассматривая доводы истца о том, что он не давал согласия на подключение услуги «Мобильный банк» и не получал ни каких СМС-извещений о списании с его счета денежных **средств** , суд исходит из следующих положений действующего законодательства, а также обстоятельств, установленных по настоящему делу:
В силу ст. 848 ГК РФ банк обязан совершать для клиентов операции, предусмотренные для счетов данного вида законом, установленными в соответствии с ним банковскими правилами и применяемыми в банковской практике обычаями делового оборота, если договором банковского счета не предусмотрено иное.
На основании ст. 854 Гражданского кодекса РФ списание денежных **средств** со счета осуществляется банком на основании распоряжения клиента. Без распоряжения клиента списание денежных **средств** , находящихся на счете, допускается по решению суда, а также в случаях, установленных законом или предусмотренных договором между банком и клиентом.

В соответствии с п. п. 1.5, 2.10 Положения Центрального Банка РФ от 24 декабря 2004 г. № 266-П «Об эмиссии банковских **карт** и об операциях, совершаемых с использованием платежных **карт** » **кредитная карта** как электронное **средство** платежа используется для совершения ее держателем операций за счет денежных **средств** , предоставленных **кредитной** организацией - эмитента клиенту в пределах расходного лимита в соответствии **с** условиями **кредитного** договора. Клиенты могут осуществлять операции с использованием платежной **карты** посредством кодов, паролей в рамках процедур их ввода, применяемых в качестве аналога собственноручной подписи и установленных **кредитными** организациями в договорах с клиентами.
Частью 15 ст. 9 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» предусмотрены основания возмещения оператором по переводу денежных **средств** клиенту суммы операции, совершенной без согласия клиента до момента направления клиентом - физическим лицом уведомления. Оператор по переводу денежных **средств** обязан возместить сумму операции, совершенной без согласия клиента, если не докажет, что клиент нарушил порядок использования электронного **средства** платежа, что повлекло совершение операции без согласия клиента – физического лица.

Как установлено выше, ДД.ММ.ГГГГ истец обратился с заявлением к ответчику на получение международной **кредитной** банковской **карты** Visa Gold **с кредитным** лимитом 50000 руб. сроком на 3 года, процентной ставкой 17,9 % годовых, в связи с чем банк на имя истца открыл счет № и выдал **кредитную карту** №.
В период времени ДД.ММ.ГГГГ ДД.ММ.ГГГГ неустановленное лицо тайно **похитило с** банковской **карты** , принадлежащей Гаврилову О.М. денежные **средства** в размере 48000 руб., отсутствие которых Гаврилов О.М. обнаружил

ДД.ММ.ГГГГ По данному факту СУ МУ МВД России «Орехово-Зуевское» возбуждено уголовное дело №, производство по которому приостановлено в связи с не установлением лица, совершившего данное преступление.

Перевод данных денежных **средств** осуществлен на различные номера телефонов, при этом три операции по 7000 руб. каждая (ДД.ММ.ГГГГ ДД.ММ.ГГГГ) осуществлены на номер телефона ДД.ММ.ГГГГ, указанный истцом в заявление на получение **кредитной карты**, принадлежащий его матери.

Списание денежных **средств с кредитной карты** истца стало возможным в результате сообщения им номеров банковских **карт** третьему лицу, подключения услуги «Мобильный банк» к указанному им номеру телефона и фактического подтверждения согласия на перечисление денежных **средств** со своей банковской **карты** верным введением ПИН-кода, являющегося аналогом собственноручной подписи, либо с использованием при входе в систему «Сбербанк Онлайн» правильных логина и одноразовых паролей, направлявшихся на подключенный к услуге «Мобильный банк» телефоны.

Исследованными в судебном заседании доказательствами не установлено вины ПАО «Сбербанк России» в причинении клиенту ущерба.

При этом в судебном заседании установлено, что истец был ознакомлен с условиями выпуска и обслуживания **кредитной карты** ОАО «Сбербанк России», тарифами ОАО «Сбербанк России», Памяткой держателя, Руководством по использованию услуг «Мобильного банка», что подтверждается его подписью об этом в заявлении на получение международной **карты** от ДД.ММ.ГГГГ и Информацией о полной стоимости **кредита** от ДД.ММ.ГГГГ Ссылки стороны истца на то, что банком не была обеспечена должная безопасность операций клиента с использованием электронного **средства** платежа, по мнению суда, несостоятельны, поскольку все выполненные ПАО «Сбербанк России» операции были осуществлены на основе полученных через платежную систему авторизационных запросов, содержание которых позволяло идентифицировать клиента. Поскольку денежные **средства** Гавриловым О.М. не были заблокированы, а их размер позволял выполнить запрашиваемые операции, оснований для отказа в совершении таких операций у банка не имелось.

Часть 9 ст. 8 Федерального закона «О национальной платежной системе» закрепляет право клиента отозвать свое распоряжение о переводе денежных **средств** до наступления безотзывности перевода в порядке, установленном законодательством и договором с оператором электронных денежных **средств** . При этом, в отношении перевода электронных денежных **средств** действует правило, установленное ч. ч. 10, 15 ст. 7 данного Федерального закона: безотзывность перевода электронных денежных **средств** наступает после осуществления оператором электронных денежных **средств** одновременного принятия распоряжения клиента, уменьшения остатка электронных денежных **средств** плательщика и увеличения остатка электронных денежных **средств** получателя **средств** на сумму перевода электронных денежных **средств.** Поскольку указанные выше операции по списанию денежных **средств** были осуществлены в режиме реального времени, о завершении операций банк надлежаще информировал истца с указанием уменьшения остатка денежных**средств** на его счете, безотзывность перевода денежных **средств** , обозначающая отсутствие или прекращение возможности отзыва распоряжения об осуществлении перевода денежных **средств** в определенный момент времени, наступила уже

ДД.ММ.ГГГГ, т.е. до обращения истца в банк, в связи с чем оснований для возложения на ответчика ответственности в виде возмещения ущерба или признания незаконной начисления указанной в иске задолженности, суд не находит. На основании ст. 56 ГПК РФ каждая сторона должна доказать те обстоятельства, на которые она ссылается как на основания своих требований и возражений, если иное не предусмотрено федеральным законом. Довод Гаврилова О.М. о том, что он не заключал с банком договор на подключение услуги «Мобильный банк» судом признается несостоятельным, поскольку в нарушение положений ст. 56 ГПК РФ суду не было представлено доказательств, отвечающих требованиям относимости и допустимости, в его подтверждение. Наоборот, согласно заявлению Гаврилова О.М. на получение**кредитной карты** от ДД.ММ.ГГГГ, указанный им номер мобильного телефона № был зарегистрирован и подключен к услуге «Мобильный банк», и сам Гаврилов О.М. не оспаривал, что **карта** постоянно находилась у него. Таким образом, суд пришел к выводу о том, что списание денежных **средств** со счета Гаврилова О.М. было осуществлено предусмотренным договором способом, в соответствии с установленными банковскими правилами и договором, а поэтому у банка имелись основания полагать, что распоряжение на снятие денежных **средств** дано уполномоченным лицом. Доказательств того, что в действиях банка имеются нарушения условий использования банковской **карты,** в материалах дела отсутствуют. С учетом совокупности представленных по делу доказательств, суд пришел к выводу о том, что истец был уведомлен и ознакомлен с условиями пользования услугой «Мобильный банк», воспользовался данной услугой, допустимых доказательств того, что списание денежных **средств с** банковской **карты** происходило в связи с неправомерными действиями Банка или третьих лиц, суду не представлено. При таких обстоятельствах, правовые основания для возложения на банк ответственности за списание **с** банковской **карты** истца денежных **средств** - отсутствуют. Ссылка на то, что в заявлении на предоставление **кредита** истец не указывал номер своего мобильного телефона, и по его заявлению вынесено постановление о возбуждении уголовного дела по факту тайного **хищения** денежных **средств с** банковской **карты,** также не является бесспорным и достаточным основанием для признания обоснованности встречных исковых требований. Согласно п. 7.14 Условий выпуска и обслуживания **кредитной карты** ОАО «Сбербанк России» предоставления услуг «Мобильного банка» осуществляется на основании полученного Банком распоряжения в виде СМС-сообщения, направленного **с** использованием **средства** мобильной связи и содержащего номер телефона, указанного держателем. При таких обстоятельствах с учетом условий договора, заключенного между сторонами, суд не находит оснований для удовлетворения заявленного иска.

На основании изложенного, руководствуясь ст.ст. 421, 848, 854 ГК РФ, ст.ст. 195-198 ГПК РФ,

РЕШИЛ:

Исковое заявление Гаврилова О.М. к ПАО «Сбербанк России» о расторжении договора банковского счета **кредитной карты** №, признании незаконным начисления задолженности по **кредитной карте** за период с ДД.ММ.ГГГГ по ДД.ММ.ГГГГ в размере 44265 руб. 55 коп. незаконным, взыскании с ответчика компенсации морального вреда 30000 руб. и судебных расходов – оставить без удовлетворения. Решение может быть обжаловано в Московский областной суд через Орехово-Зуевский

городской суд путем подачи апелляционной жалобы в течение месяца со дня принятия решения суда в окончательной форме.

Судья: И.Н. Щипанов

Мотивированное решение составлено 31 мая 2018 года

- **Решение № 2-2039/2018 2-2039/2018 ~ М-1439/2018 М-1439/2018 от 23 мая 2018 г. по делу № 2-2039/2018**

Новгородский районный суд (Новгородская область) – Гражданские и административные

Дело № 2-2039/2018

РЕШЕНИЕ

именем Российской Федерации 23 мая 2018 года город Великий Новгород Новгородский районный суд Новгородской области в составе: председательствующего судьи Зуева Н.В., при секретаре Новожиловой Д.А., с участием представителя истца Курбанисмаиловой Х.М., рассмотрев в открытом судебном заседании гражданское дело по иску Степановой ФИО5 к акционерному обществу «Бинбанк Диджитал» о взыскании неправомерно списанных денежных **средств**,

установил:

Степанова Г.Н. обратилась в Новгородский районный суд с иском к АО «Бинбанк» (далее – Банк) о взыскании неправомерно списанных денежных **средств,** указав, что 13.01.2015 г. между Степановой Г.Н. и Банком был заключен **кредитный** договор о предоставлении банковских услуг, согласно которому была выпущена банковская **карта с кредитным** лимитом 200 000 рублей. 12.02.2018 г. на мобильный телефон истца пришло СМС-сообщение о том, что **с** банковской **карты** списан 7 500 рублей, инф. №. Перезвонив по указанному номеру, ей представились сотрудниками Банка, после этого было проведено пять транзакций на общую сумму 138 163 руб. 26 коп., комиссия 2 589 руб. 30 коп. 13.02.2018 г. Степанова Г.Н. обратилась в Банк с письменным заявлением о возврате денежных **средств,** а также в правоохранительные органы о незаконном снятии **с карты** денежных **средств.** Банк отказал в возврате денег, а органами следствия возбуждено уголовное дело. Считает, что отказ Банка о возврате денежных **средств** является необоснованным и незаконным. Просит аннулировать операции по списанию **кредитных средств** и вернуть неправомерно списанные денежные **средства** в размере 140 752 руб. 56 коп.

Истец в судебное заседание не явилась, извещена надлежащим образом, представила заявление о рассмотрении дела без своего участия.

Представитель истца поддержала требования в полном объеме.

Представитель Банка в судебное заседание не явился, о рассмотрении дела извещен надлежащим образом, просил рассмотреть без своего участия, иск не признает по мотивам, изложенным в отзыве на иск.

Выслушав представителя истца, исследовав письменные материалы дела, суд приходит к следующему.

Согласно ст. 845 ГК РФ по договору банковского счёта банк обязуется принимать и зачислять поступающие на счёт, открытый клиенту (владельцу счёта), денежные **средства** , выполнять распоряжения клиента о перечислении и выдаче соответствующих сумм со счёта и проведении других операций по счёту. Банк не вправе определять и контролировать направления использования денежных **средств** клиента и устанавливать другие, не предусмотренные законом или договором банковского счёта ограничения его права распоряжаться денежными **средствами** по своему усмотрению.

В силу ст. 847 ГК РФ права лиц, осуществляющих от имени клиента распоряжения о перечислении и выдаче **средств** со счёта, удостоверяются клиентом путём представления банку документов, предусмотренных законом, установленными в соответствии с ним банковскими правилами и договором банковского счёта. Договором может быть предусмотрено удостоверение прав распоряжения денежными суммами, находящимися на счёте, электронными **средствами** платежа и другими документами с использованием в них аналогов собственноручной подписи (пункт 2 статьи 160), кодов, паролей и иных **средств**, подтверждающих, что распоряжение дано уполномоченным на это лицом.

Исходя из положений ст. 849 ГК РФ следует, что банк обязан по распоряжению клиента выдавать или перечислять со счёта денежные **средства** клиента не позже дня, следующего за днём поступления в банк соответствующего платёжного документа, если иные сроки не предусмотрены законом, изданными в соответствии с ним банковскими правилами или договором банковского счёта.

Согласно п. 15 ст. 9 Федерального закона «О национальной платежной системе» от 27.06.2011 г. № 161-ФЗ в случае, если оператор по переводу денежных **средств** исполняет обязанность по уведомлению клиента - физического лица о совершенной операции в соответствии с частью 4 настоящей статьи и клиент - физическое лицо направил оператору по переводу денежных **средств** уведомление в соответствии с частью 11 настоящей статьи, оператор по переводу денежных **средств** должен возместить клиенту сумму указанной операции, совершенной без согласия клиента до момента направления клиентом - физическим лицом уведомления. В указанном случае оператор по переводу денежных **средств** обязан возместить сумму операции, совершенной без согласия клиента, если не докажет, что клиент нарушил порядок использования электронного **средства** платежа, что повлекло совершение операции без согласия клиента – физического лица.

Как следует из материалов дела, на основании анкеты-заявления о присоединении к Условиям и Правилам предоставления банковских услуг от 18.03.2015 г. Степановой Г.Н. был открыт счет № № и выдана **кредитная карта.**

В судебном заседании установлено, что 12 февраля 2018 года на мобильный телефон истца (указан в анкете-заявлении) с номера телефона 950 451 04 39 поступило СМС-сообщение следующего содержания: «списание **с** вашей **карты** 7 500 рублей».

Как следует из протокола принятия устного заявления о преступлении, Степанова Г.Н. позвонила по телефону №, где ей представились сотрудниками службы безопасности Банка и сказали, что в Банке произошел сбой и попросили для решения проблем назвать цифры, которые придут в сообщениях. Далее на мобильный телефон стали приходить СМС-

сообщения, текст которых Степанова Г.Н. сообщала по телефону №. Так происходило 7 или 8 раз, после чего ей сказали выключить телефон на 3 часа.

Согласно детализации по телефонному номеру Степановой Г.Н., входящее СМС-сообщение с телефона № поступило 12.02.2018 г. в 13 час. 15 мин., затем в 13 час. 41 мин. был произведен исходящий звонок на вышеуказанный номер. В 13 час. 50 мин., в 13 час. 51 мин., в 13 час. 55 мин., 14 час. 00 мин. (2 сообщения), 14 час. 02 мин., в 14 час. 04 мин. (2 сообщения), 14 час. 05 мин., в 14 час. 07 мин. (2 сообщения), в 14 час. 09 мин., в 14 час. 10 мин. (2 сообщения), в 14 час. 12 мин., в 14 час. 13 мин., в 14 час. 14 мин., в 14 час. 15 мин., в 14 час. 16 мин. (2 сообщения), в 14 час. 17 мин., в 14 час. 18 мин. (2 сообщения), в 14 час. 19 мин. и в 15 час. 25 мин. отражены входящие СМС-сообщения от Банка. В 13 час. 52 мин., в 13 час. 53 мин., в 13 час. 54 мин., в 13 час. 57 мин., в 13 час. 59 мин., в 14 час. 06 мин., в 14 час. 09 мин., в 14 час. 11 мин., в 14 час. 15 мин., в 14 час. 17 мин., в 14 час. 19 мин. и в 15 час. 08 мин. отражены входящие звонки с номера 992 204 47 34. В 13 час. 55 мин., в 14 час. 02 мин. в 14 час. 05 мин. исходящий звонок на номер 992 204 47 34. В 14 час. 22 мин. и в 15 час. 23 мин. исходящие звонки на телефон 8 800 200 20 80.

Из представленной ответчиком информации следует, что на телефон Степановой Г.Н. от Банка были направлены СМС-сообщения в 13 час. 50 мин. с текстом: «Код № для расходной операции по **карте** на сумму 22 222 руб. сайт <данные изъяты>. Никому не сообщайте код во избежание мошенничества! Телефон банка 8 800 указан на **карте** », в 13 час. 55 мин. с текстом: «Перевод на **карту** *7501: 22555.33 RUR 12.02.18 13:55. Баланс: 115889.16 RUR.i.binbank.ru», в 14 час. 00 мин. с текстом: «Код № для расходной операции по **карте** *4975 на сумму 56 110.55 RUR сайт <данные изъяты>. Никому не сообщайте код во избежание мошенничества! Телефон банка 8 800 указан на**карте** », в 14 час. 02 мин. с текстом: «Перевод на **карту** : 56110.55 RUR 12.02.18 14:02. Баланс: 59778.61 RUR.i.binbank.ru», в 14 час. 07 мин. с текстом: «Код № для расходной операции по **карте** *4975 на сумму 33 333.00 RUR сайт <данные изъяты>. Никому не сообщайте код во избежание мошенничества! Телефон банка 8 800 указан на **карте** », в 14 час. 09 мин. с текстом: «Перевод на **карту** *4760: 33966.33 RUR 12.02.18 14:09. Баланс: 25812.28 RUR.i.binbank.ru», в 14 час. 10 мин. с текстом: «Код № для расходной операции по **карте** *4975 на сумму 15 555.00 RUR сайт <данные изъяты>. Никому не сообщайте код во избежание мошенничества! Телефон банка 8 800 указан на**карте** », в 14 час. 12 мин. с текстом: «Перевод на **карту** *4760: 15850.55 RUR 12.02.18 14:12. Баланс: 9961.73 RUR.i.binbank.ru», в 14 час. 13 мин. с текстом: «Код № для расходной операции по **карте** *4975 на сумму 9500.00 RUR сайт <данные изъяты>. Никому не сообщайте код во избежание мошенничества! Телефон банка 8 800 указан на **карте** », в 14 час. 15 мин. с текстом: «Перевод на **карту** *4760: 9680.50 RUR 12.02.18 14:15. Баланс: 281.23 RUR.i.binbank.ru», в 15 час. 25 мин. **с** текстом: « **Карта** VISA *4975 заблокирована 12-02-18 15:25:42. <данные изъяты>! Телефон №

Из представленной информации, следует также, что всем операциям по переводу денежных **средств** были присвоены номера авторизации.

13.02.2018 г. Степанова Г.Н. обратилась в Банк с заявлением о несогласии с транзакциями от 12.02.2018 г. на суммы операций 56 110,55 руб., 33 966,33 руб., 9680,50 руб., 15850,55 руб. и 22 555,33 руб.

12.02.2018 г. Степанова Г.Н. обратилась в правоохранительные органы, где 22.02.2018 г. возбудили уголовное дело № № по преступлению, предусмотренному ч. 1 ст. 159 УК РФ. Постановлением от 01.06.2018 г. Степанова Г.Н. признана потерпевшей по уголовному делу. Постановлением от 07.03.2018 г. Степанова Г.Н. признана гражданским истцом по уголовному делу.

Согласно анкеты-заявления Степанова Г.Н. ознакомлена с Условиями обслуживания банковских **карт** платежных **карт** физических лиц как электронного **средства** платежа Банка, Правилами пользования банковскими **картами,** Тарифы, утвержденные Банком.

Пунктом 4.11 Общих условий выпуска и обслуживания банковских расчетных (дебетовых) **карт с кредитным** лимитом установлено, что клиент обязан уведомить Банк об утрате **карты** и/или обнаружения факта использования **карты** без своего согласия, немедленно, но не позднее дня, следующего за днем получения уведомления от Банка, в порядке, предусмотренном п. 23 Условий. Невыполнение данной обязанности освобождает Банк от обязанности по возмещению клиенту денежных **средств** в случае использования **карты** без согласия клиента.

Из пункта 5.5 Условий следует, что Банк имеет право отказать клиенту в возмещении суммы операции, совершенной без согласия клиента, в случае, если клиент не уведомил Банк об утрате **карты** и(или) использования **карты** без согласия клиента в порядке, предусмотренном п. 23 Условий.

Согласно п. 23 Условий в случае утраты **карты** и(или) обнаружения факта использования **карты** без своего согласия клиент посредством обращения в ЕИЦ Банка уведомляет Банк о данных фактах с целью блокировки **карты.** Обращение в ЕИЦ Банка возможно круглосуточно. После обращения в ЕИЦ Банка клиент обязан предоставить в Банк письменное заявление в порядке и срок, установленный п. 24.1-24.3 Условий. Обращение в ЕИЦ не является заявлением клиента о факте утраты **карты** и (или) использования е без согласия клиента и не является основанием для возмещения денежных **средств,** списанных со счета без согласия клиента.

В соответствии с п. 6.10 Условий Банк, при совершении клиентом в сети Интернет операций 3Ds с помощью реквизитов **карты** вправе до начала выполнения клиентом таких операций 3Ds предложить на специальной странице Банка в сети Интернет ввести персональный одноразовый код с целью проведения дополнительной аутентификации. Отказать в совершении операций 3Ds, если клиент отказался ввести на специальной странице Банка в сети Интернет персональный одноразовый код с целью проведения дополнительной аутентификации в соответствии с п. 6.10.1 Условий и/или ввел на специальной странице в сети Интернет код, не соответствующий персональному одноразовому коду, направленному Банком клиенту в соответствии с п. 6.10.1.

Банк освобождается от обязанности возмещать сумму операции, совершенной без согласия клиента, в случае нарушения клиентом Правил (п. 27.2 и 27.2.2 Условий).

В соответствии с п. 6.3 Правил пользования банковскими **картами** при совершении операций **с** использованием **карты** через сеть Интернет держатель **карты** должен не сообщать свои персональные данные или информацию о **карте** через сеть Интернет, например, ПИН-код, кодовое слово, пароли доступа к ресурсам Банка, историю операций т.п.

Пунктами 7.2.3 и 7.2.4 Правил запрещено передавать **карту** и сообщать ПИД-код третьим лицам. Использование **карты** третьим лицом незаконно и рассматривается Банком как грубое нарушение настоящих Правил и может повлечь за собой расторжение договора по инициативе Банка. Запрещается сообщать кому-либо номер **карты.**

Пункт 5.5. Условий обслуживания банковских счетов и платежных **карт** физических лиц как электронного **средства** платежа содержит аналогичные условия, как и пункт 6.4 Общих условий выпуска и обслуживания банковских расчетных (дебетовых) **карт с кредитным** лимитом.

Таким образом, в судебном заседании установлены нарушения вышеуказанных Условий и Правил самой Степановой Г.Н.

Как указал Конституционный Суд РФ в своём определении от 25.02.2016 г. № 428-О правовое регулирование использования электронных**средств** платежа осуществляется в соответствии с Федеральным законом от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе». Согласно части 15 статьи 9 данного Федерального закона в случае, если оператор по переводу денежных **средств** исполняет обязанность по уведомлению клиента – физического лица о совершенной операции с использованием электронного **средства** платежа и клиент – физическое лицо в установленном данной статьей порядке направил оператору по переводу денежных **средств** уведомление об использовании электронного **средства** платежа без его согласия, оператор по переводу денежных **средств** должен возместить клиенту сумму указанной операции, совершенной без согласия клиента до момента направления клиентом - физическим лицом уведомления; в указанном случае оператор по переводу денежных **средств** обязан возместить сумму операции, совершенной без согласия клиента, если не докажет, что клиент нарушил порядок использования электронного **средства** платежа, что повлекло совершение операции без согласия клиента – физического лица. Применяемый во взаимосвязи с этими нормативными положениями пункт 4 статьи 13 Закона Российской Федерации «О защите прав потребителей» с учетом разъяснения, содержащегося в пункте 28 Постановления Пленума Верховного Суда Российской Федерации от 28 июня 2012 года № 17 «О рассмотрении судами гражданских дел по спорам о защите прав потребителей», о том, что при разрешении требований потребителей необходимо учитывать, что бремя доказывания обстоятельств, освобождающих от ответственности за неисполнение либо ненадлежащее исполнение обязательства, в том числе и за причинение вреда, лежит на продавце (изготовителе, исполнителе, уполномоченной организации или уполномоченном индивидуальном предпринимателе, импортере) (пункт 4 статьи 13, пункт 5 статьи 14, пункт 5 статьи 23.1, пункт 6 статьи 28 Закона о защите прав потребителей, статья 1098 ГК Российской Федерации), не содержит неопределенности, поскольку допускает возможность освобождения оператора по переводу денежных **средств**от предусмотренной Федеральным законом «О национальной платежной системе» обязанности возместить клиенту сумму операции, совершенной с использованием электронного **средства** платежа до направления клиентом оператору по переводу денежных **средств**уведомления об использовании электронного **средства** платежа без его согласия, лишь при предоставлении им (оператором) доказательств нарушения порядка использования электронного **средства** платежа клиентом, повлекшего совершение данной операции.

При таких обстоятельствах, учитывая, что все перечисленные выше операции были осуществлены в рамках установленных Условий и Правил, согласованных между АО «Бинбанк» и Степановой Г.Н. на основании её заявления, а также то, что истец в нарушение Условий и Правил использования банковскими **картами** АО «Бинбанк» лично передала третьим лицам информацию, оснований для удовлетворения заявленных требований о взыскании денежных **средств** , не имеется.

Законные основания для отказа в совершении расходных операций по счету Степановой Г.Н. у Банка отсутствовали, так как согласно ст. 845 ГК РФ банк не вправе определять и контролировать направления использования денежных **средств** клиента и устанавливать другие, не предусмотренные законом или договором, ограничения его права распоряжаться денежными **средствами** по своему усмотрению. Ни ГК РФ, ни Правила, регулирующие данные правоотношения, не требуют от банков проведения специальных мер по установлению подлинности **карты**.

Следовательно, означенные операции по списанию денежных **средств** следует считать совершенными самим держателем **карты**(ответчиком) либо по его распоряжению. Операции по списанию денежных **средств** со счета истца были проведены Банком правомерно, в соответствии с законодательством, нормативными актами и условиями заключенного между сторонами договора.

Никаких доказательств наличия вины Банка в списании денежных **средств** ответчиком не представлено.

Кроме того, ни законом, ни условиями заключенного между сторонами договора не предусмотрены обязательства банка по контролю за несанкционированным доступом к счету клиента, а также ответственность банка за несанкционированное списание денежных **средств с кредитной карты.**

Несанкционированный доступ к счету истца имел место не по причине ненадлежащего оказания ответчиком банковской услуги, а вследствие противоправных действий неустановленных лиц.

Противоправные действия третьих лиц являются основанием для их гражданско-правовой ответственности перед истцом по обязательствам вследствие причинения вреда либо неосновательного обогащения, но не гражданско-правовой ответственности ответчика за несоблюдение (ненадлежащее соблюдение) условий заключенного сторонами договора. Банк обязан производить списание денежных**средств** по указанию клиента, при этом банк не вправе проводить оперативно-розыскные мероприятия по проверке обстоятельств получения указания клиента.

В случае установления приговором суда лица, виновного в **хищении** денежных **средств** со счета истца, она не лишена возможности возместить нанесенный ущерб за счет непосредственного причинителя ущерба.

Руководствуясь ст.ст.194-199 ГПК РФ, суд

решил:

Исковые требования Степановой ФИО6 к акционерному обществу «Бинбанк Диджитал» о взыскании неправомерно списанных денежных**средств** оставить без удовлетворения.

Решение может быть обжаловано в Судебную коллегию по гражданским делам Новгородского областного суда через Новгородский районный суд в течение месяца со дня составления мотивированного решения 24 мая 2018 года.

Председательствующий Зуев Н.В.

Мотивированное решение изготовлено 24.05.2018 г.

5.3.2. Решения по искам о возмещении денежных средств, несанкционированно списанных с кредитной карты.

Решение № 2-5708/2017 2-624/2018 от 8 февраля 2018 г. по делу № 2-5708/2017

Свердловский районный суд г. Костромы (Костромская область) – Гражданские и административные

Дело № 2-624/2018

РЕШЕНИЕ

ИМЕНЕМ РОССИЙСКОЙ ФЕДЕРАЦИИ

08 февраля 2018 года

Свердловский районный суд г. Костромы в составе

судьи Комиссаровой Е.А.

при секретаре Корневой Л.П.

рассмотрев в открытом судебном заседании гражданское дело по иску ПАО «Сбербанк России» в лице филиала- Костромского отделения № 8640 к Максимовой Виктории Владимировне о взыскании ссудной задолженности по банковской карте и по встречному иску Максимовой Виктории Владимировны к ПАО «Сбербанк России» о взыскании компенсации морального вреда,

у с т а н о в и л :

Истец обратился с выше указанным иском, обосновав тем, что на основании личного заявления от <дата> Максимова В.В. получила **кредитную карту** №, выпущенную ПАО Сбербанк с **лимитом** на сумму 39848,14 руб. под 24 % годовых, начиная с <дата> заемщик не исполняет свои обязательства по **кредитному** договору, по ежемесячному погашению **кредита** и уплате процентов за пользование **кредитом**. Согласно п. 3.3 Условия выпуска и обслуживания **кредитной карты** Сбербанка России операции, совершаемые с использованием **карт**, относятся на счет **карты** и оплачиваются за счет **кредита** , предоставленного держателю, с одновременным уменьшением доступа **лимита** . Пунктом 3.5 Условий предусмотрено, что проценты начисляются на даты отражения операции по ссудному счету до даты погашения задолженности (включительно). При исчислении процентов за пользование **кредитом** в расчет принимаются фактическое количество календарных дней в платежном периоде, в году – действительное число календарных дней. В соответствии с п. 4.1.3 Условий Держатель **карты** обязан ежемесячно до наступления даты платежа пополнить счет **карты** на сумму обязательного платежа, указанную в отчете для погашения задолженности. По состоянию на <дата> обязательства по Договору не исполняются надлежащим образом, допущена просрочка платежа в количестве 253 дня. Согласно п 5.2.8 Условий Банк имеет право при нарушении

Держателем настоящих условий или при возникновении ситуации, которая может повлечь за собой ущерб для Банка или Держателя, либо нарушение действующего законодательства: приостановить или досрочно прекратить действие **карты,** а также принимать для этого все необходимые меры вплоть до изъятия **карты**; направить Держателю уведомление с требованием досрочной оплаты суммы общей задолженности по**карте** и возврата **карты** в Банк. По состоянию на <дата> задолженность составляет 47851,86 руб.

Ответчик Максимова В.В. заявила встречные требования, в которых просит отказать в удовлетворении требований истца, взыскать в ее пользу компенсацию морального вреда, причиненного незаконными действиями Банка, обосновав тем, что на основании заявления она получила банковскую **карту** с первоначальным **лимитом** 10000 руб., в последствии этот **лимит** ей был увеличен, ей был подключен мобильный банк, однако заявление на него она не писала, <дата> она проверила баланс своего телефона и обнаружила там сумму 14000 руб., в этот же день она обратилась в ТЕЛЕ 2 и в офис Сбербанк, где ей разъяснили, что в отношении нее совершены мошеннические действия, **карту** при ней уничтожили, потом она написала заявление на **восстановление лимита** и о выдаче выписки по счету, по факту мошенничества она обратилась в ОП 3 УМВД России по г. Костроме, деньги в сумме 14000 руб. ей вернули, она отнесла их в Сбербанк в счет погашения долга по **кредитной карте** , <дата> она получила ответ Сбербанка с отказом в **восстановлении лимита** . Она обращалась с заявлением о снятии с нее долговых обязательств в связи с мошенническими действиями, но получила отказ. Свою **кредитную карту**она никому не передавала, пин-кода не сообщала, тем самым не нарушала условий использования банковской **карты.** Услуги Банка по обслуживанию счета должны быть безопасными для сохранения денежных средств. Банк не предоставил документов, что она нарушила порядок использования электронного средства платежа. Факт незаконного **списания** с ее **карты** денежных средств установлен и подтвержден. Банк обязан взыскивать денежные средства с лиц, которые своими мошенническими действиями причинили вред путем незаконного **списания** с **кредитной карты** денежных средств.

В ходе рассмотрения дела встречный иск ответчиком был уточнен, просила взыскать компенсацию морального вреда в сумме 35 000 рублей по указанным выше основаниям.

Представитель истца в судебном заседании иск поддержала в полном объеме, против удовлетворения встречного иска возражала, поддержала письменные возражения.

Ответчик Максимова В.В. в судебном заседании и ее представитель иск не признали, поддержали встречный иске, уточнив, что неправомерными действиями банка, причинившими ей физические и нравственные страдания считает отказ в пополнении **кредитного лимита** на сумму похищенных денежных средств, многочисленные судебные тяжбы, поскольку банк инициирует иски, хождение в полицию, в то время как именно Банк должен был заявлять о хищении денежных средств, которые находились на **кредитной карте** , поскольку данные денежные средства являются собственностью Банка. Считают, что Банк не доказал виновность Максимовой В.В.

Представитель третьего лица ООО «Т2 Мобайл» в судебное заседание не явился, извещены надлежащим образом, просили рассмотреть дело в отсутствии представителя.

Исследовав материалы дела, выслушав представителя истца, ответчика и ее представителя, суд приходит к следующему.

Согласно статье 309 Гражданского кодекса Российской Федерации обязательства должны исполняться надлежащим образом в соответствии с условиями обязательства и требованиями закона, иных правовых актов, а при отсутствии таких условий и требований – в соответствии с обычаями делового оборота или иными обычно предъявляемыми требованиями.

В соответствии со статьей 819 Гражданского кодекса Российской Федерации по **кредитному** договору банк иная **кредитная** организация (кредитор) обязуются предоставить денежные средства (**кредит**) заемщику в размере и на условиях, предусмотренных договором, а заемщик обязуется возвратить полученную денежную сумму и уплатить проценты на нее.

Из пункта 2 статьи 811 Гражданского кодекса Российской Федерации следует, что, если договором займа предусмотрено возвращение займа по частям (в рассрочку), то при нарушении заемщиком срока, установленного для возврата очередной части займа, заимодавец вправе потребовать досрочного возврата всей оставшейся суммы займа вместе с причитающимися процентами.

Судом установлено, что на основании личного заявления от <дата> Максимовой В.В. была выдана **кредитная карта** № с **лимитом** на сумму 10000 руб., срок **кредита** 36 месяцев, процентная ставка по **кредиту** 24 % годовых.

В соответствии с пунктом 1.1 Условий выпуска и обслуживания **кредитной карты** ПАО Сбербанк настоящие условия выпуска и обслуживания **кредитной карты** ПАО Сбербанк в совокупности с Памяткой Держателя **карт** ПАО Сбербанк, Памяткой по безопасности при использовании **карт** , Заявлением на получение **карты** , надлежащим образом заполненным и подписанным Клиентом, Альбомом тарифов на услуги, предоставляемые ПАО Сбербанк физическим лицам, являются заключенным между Клиентом и ПАО Сбербанк Договором на выпуск и обслуживание банковской **карты** , открытие Счета для учета операций с использованием **карты** , и предоставление Держателю возобновляемой **кредитной** линии для проведения операций по **карте** .

Как следует из заявления на получение банковской **карты** Максимова В.В. была ознакомлена с «Условиями использования **карт**», Памяткой Держателя и Тарифами Сбербанка России, согласилась с ними, обязалась их выполнять.

В случае несвоевременного внесения обязательного платежа взимается неустойка в соответствии с Тарифами банка (пункт 3.9 Условий выпуска и обслуживания **кредитной карты** Сбербанка России).

Поскольку заемщик перестала исполнять принятые на себя обязательства по внесению ежемесячных платежей по погашению **кредита** и начисленных процентов, что в соответствии с законом и условиями **кредитного** договора предоставляет банку право досрочно требовать возврата всей суммы **кредита**, банк обратился в суд с настоящим иском.

В соответствии со ст.819 ГК РФ по **кредитному** договору банк или иная **кредитная** организация (кредитор) обязуются предоставить денежные средства (**кредит**) заемщику в размере и на условиях, предусмотренных договором, а заемщик обязуется возвратить полученную денежную сумму и уплатить проценты на нее.

К отношениям по **кредитному** договору применяются правила, предусмотренные параграфом 1 (Заем) настоящей главы, если иное не предусмотрено правилами настоящего параграфа и не вытекает из существа **кредитного** договора.

В силу п. 1 ст. 810 ГК РФ заемщик обязан возвратить займодавцу полученную сумму займа в срок и в порядке, которые предусмотрены договором займа.

В соответствии с п. 4.1.1 Условий выпуска и обслуживания **кредитной карты** Ответчик обязан выполнять положения настоящих Условий, требования Памятки Держателя, Памятки по безопасности.

В соответствии с п. 4.1.3 Условий Держатель **карты** обязан ежемесячно до наступления даты платежа пополнить счет **карты** на сумму обязательного платежа. Указанную в отчете для погашения задолженности.

В соответствии с п. 5.2.8 Условий Банк имеет право при нарушении Держателем настоящих условий или при возникновении ситуации, которая может повлечь за собой ущерб для Банка или Держателя, либо нарушении действующего законодательства: приостановить или досрочно прекратить действие **карты**, а так же принимать для этого все необходимые меры вплоть до изъятия **карты**; направить Держателю **карты** уведомление с требованием досрочной оплаты суммы общей задолженности по **карте** и возврата **карты** в Банк.

О необходимости осуществления необходимых платежей по **карте** ответчик извещалась путем направления требования.

Как установлено в судебном заседании, ответчик Максимова В.В. свои обязательства по указанному договору ненадлежащим образом не выполняла.

По состоянию на <дата> сумма задолженности ответчика перед истцом составляет 39848,14 – просроченный основной долг; 5906,02 руб. – просроченные проценты; 2097,7 руб. – неустойка.

Указанные суммы подлежат взысканию с ответчика в пользу истца.

Представленный Банком расчет **кредитной** задолженности, произведенный в соответствии с условиями предоставления **карты**, судом проверен и признан правильным.

При таких обстоятельствах суд считает требования истца о взыскании с ответчика образовавшейся задолженности по **кредиту** законными, обоснованными и подлежащими удовлетворению.

Также в соответствии со ст. 98 ГПК РФ суд считает необходимым взыскать с ответчика расходы в виде уплаченной государственной пошлины в сумме 1635,56 руб.

Обращаясь со встречным иском, истица указывает на то, что действиями Банка нарушены ее права как потребителя банковской услуги. Так, Банк в отсутствие доказательств ее вины по **несанкционированному** использованию **кредитных** средств, отказался восполнить счет**кредитной карты**, похищенные денежные средства

с **карты** вынесены банком на просрочку, начислены проценты и пени, каких-либо мер по установлению лиц, совершивших хищение, возврату денежной суммы не предпринял, необоснованно возложив ответственность на нее. Данными действиями ей причинены физические и нравственные страдания, она вынуждена ходить по судам и в правоохранительные органы.

Однако суд не находит оснований для удовлетворения заявленных встречных требований по следующим основаниям.

Из материалов дела следует, что на основании заявления в ОАО Сбербанк Росси на получение **кредитной карты**, Максимова В.В. являлась держателем **кредитной** банковской **карты** VISA. При получении **карты** она была подключена к услуге "Мобильный банк" на номер телефона.

В собственноручно подписанном заявлении на выпуск указанной **карты** Максимова В.В. подтвердила, что с условиями выпуска и обслуживании **кредитной карты** ОАО "Сбербанк России", Тарифами ОАО "Сбербанк России", Памяткой Держателя, Руководством по использованию услуг "Мобильного банка" получила с условиями предоставления услуг «Мобильного банка», ознакомлена, согласна и обязуется их выполнять (л.д. 106-107).

За период с 26 октября по <дата> посредством услуги в системе «Мобильный банк» на основании СМС-сообщений с **карты** , открытой на имя Максимовой В.В., совершены операции безналичной оплаты в общей сумме 49065 руб. Банк перечислил денежные средства на основании запросов, поступивших с номера телефона +79536438289, зарегистрированного в Банке на имя Максимовой В.В.

Согласно ст. 845 ГК РФ по договору банковского счета банк обязуется принимать и зачислять поступающие на счет, открытый клиенту (владельцу счета), денежные средства, выполнять распоряжения клиента о перечислении и выдаче соответствующих сумм со счета и проведении других операций по счету. Банк не вправе определять и контролировать направления использования денежных средств клиента и устанавливать другие не предусмотренные законом или договором банковского счета ограничения его права распоряжаться денежными средствами по своему усмотрению.

Согласно части 1 статьи 854 ГК РФ **списание** денежных средств со счета осуществляется банком на основании распоряжения клиента.

Договором может быть предусмотрено удостоверение прав распоряжения денежными суммами, находящимися на счете, электронными средствами платежа и другими документами с использованием в них аналогов собственноручной подписи (пункт 2 статьи 160 ГК РФ), кодов, паролей и иных средств, подтверждающих, что распоряжение дано уполномоченным на это лицом (пункт 3 статьи 847 этого Кодекса).

Согласно ст. 848 ГК РФ банк обязан совершать для клиента операции, предусмотренные для счетов данного вида законом, установленными в соответствии с ним банковскими правилами и применяемыми в банковской практике обычаями делового оборота, если договором банковского счета не предусмотрено иное.

В соответствии с п. 15 ст. 7 ФЗ от 27.06.2011 N 161-ФЗ "О национальной платежной системе" перевод электронных денежных средств становится безотзывным и

окончательным после осуществления оператором электронных денежных средств действий, указанных в части 10 ст. 7 Закона. Согласно п. 10 ст. 7 указанного Закона перевод электронных денежных средств осуществляется путем одновременного принятия оператором электронных денежных средств распоряжения клиента, уменьшения им остатка электронных денежных средств плательщика и увеличения им остатка электронных денежных средств получателя средств на сумму перевода электронных денежных средств либо в срок, предусмотренный частью 11 настоящей статьи.

Оператор электронных денежных средств незамедлительно после исполнения распоряжения клиента об осуществлении перевода электронных денежных средств направляет клиенту подтверждение об исполнении указанного распоряжения (п. 13 Закона).

Пунктом 1.14 Положения Банка России от 24 декабря 2004 г. N 266-П "Об эмиссии банковских **карт** и об операциях, совершенных с использованием банковских **карт** " предусмотрено, что при выдаче платежной **карты**, совершении операции с использованием платежной**карты кредитная** организация обязана идентифицировать ее держателя. Идентификация осуществляется на основе реквизитов платежной (банковской) **карты**, а также кодов (паролей).

Согласно Руководству по пользованию "Мобильного банка", которое находится в открытом доступе, перевод средств на **карты** "Сбербанка" осуществляется на основании смс-сообщения, содержащего код подтверждения и реквизиты операции; совершение платежа осуществляется только после направления клиентом 5-значного кода подтверждения, на короткий №, что и имело место в рассматриваемом случае.

В соответствии с пунктами 7.14, 7.15 Условий выпуска и обслуживания **кредитной карты** предоставление услуги мобильный банк осуществляется на основании полученного Банком распоряжения в виде СМС, направленного с использованием средств мобильной связи с номера телефона, указанного держателем при подключении Мобильного банка. Держатель **карты** подтверждает, что полученное Банком сообщение рассматривается как распоряжение на проведение операции по счетам **карт** держателя.

Согласно пункту 7.21 Условий выпуска и обслуживания **кредитной карты** банк не несет ответственность за ущерб и факт разглашения банковской тайны, возникшие вследствие допуска держателем третьих лиц к использованию мобильного телефона, номер которого используется для предоставления услуги "Мобильный банк"; за последствия использования распоряжения, переданного в банк с использованием номера мобильного телефона держателя, в том числе, в случае использования мобильного телефона держателя неуполномоченным лицом.

Из протокола списка СМС-сообщений, отправленных Банком на номер мобильного телефона ответчика № следует, что с 26 октября по <дата> на телефон ответчика направлялись сообщения - одноразовый пароль для подтверждения совершаемой клиентом операции.

Направленные банком СМС-сообщения подтверждает совершение клиентом заявленной операции, путем правильного ввода одноразового пароля, высланного ранее. (л.д. 99)

Факт получения указанных сообщений подтверждается детализацией оказанных услуг по абонентскому номеру ответчика. (л.д. 164).

Полагая, что произошло **несанкционированное списание** денежных средств с **карт**, Максимова В.В. обратилась в дополнительный офис Банка, где на основании ее обращения счет был заблокирован, **карта** уничтожена. На заявление Максимовой В.В. в банк о**восстановлении лимита** она получила отказ. При повторном аналогичном обращении <дата> получила письмо банка с отказом снятия с нее долговых обязательств.

Согласно п. 4.1.6 Условий выпуска и обслуживания **кредитной карты** ОАО "Сбербанк России", держатель **карты** обязуется не сообщать ПИН-код и номер **карты**, а также не передавать **карту** (ее реквизиты) для совершения операций иным лицам, предпринимать необходимые меры для предотвращения утраты, повреждения, хищения **карты.**

Согласно п. <дата>. Условий держатель **карты** несет ответственность за операции с **Картой** (реквизитами **карты**), совершенными до момента получения банком уведомления об утрате **карты**.

В силу пункта 8.8, 8.9 Условий клиент соглашается с тем, что постоянный и одноразовый пароли являются аналогом собственноручной подписи, электронные документы, подтвержденные постоянным и/или одноразовым паролем, признаются Банком и Держателем равнозначными документами на бумажном носителе и могут служить доказательством в суде. Документальным подтверждением факта совершения клиентом операции является протокол проведения операций в автоматизированной системе банка, подтверждающий корректную идентификацию и аутентификацию держателя и совершения операции в такой системе.

В данном случае все операции были совершены посредством использования услуги "Мобильный банк" с телефона абонента ..., принадлежащего Максимовой В.В. и указанного ею при подключении услуги "Мобильный банк" к обслуживанию **кредитной карты**, путем направления смс - сообщений с последующем направлением кода для подтверждения операции.

Таким образом, у Банка не было оснований для отказа в совершении операций, совершенных в период с 26 октября по <дата>.

При этом, спорные операции совершены с 26 октября по <дата> включительно, что подтверждает мгновенное и безвозвратное **списание** Банком денежных средств со счета клиента в указанное время до обращения Максимовой В.В. с заявлением об оспаривании указанных операций.

Кроме того, денежные средства на **карте** являлись **кредитом**, предоставляемым Банком ответчику, и, следовательно, не могли быть возвращены Максимовой В.В.

Соответствующие доводы Банка и представленные им доказательства, какими-либо доказательствами со стороны ответчика не опровергнуты.

При этом каких-либо достоверных и достаточных доказательств **списания** данных денежных средств в результате неправомерных действий третьих лиц и без ведома Ответчика в материалы дела не представлены.

Доводы Максимовой В.В. о том, что находящимися на **карте** денежными средствами воспользовались третьи лица, по факту хищения денежных средств возбуждено уголовное дело, основанием к удовлетворению е требований не являются, поскольку постановление следователя не имеет преюдициального значения для разрешения настоящего спора, так как в силу положений ч. 4 ст. 61 ГПК РФ только вступивший в законную силу приговор суда по уголовному делу обязателен для суда, рассматривающего дело о гражданско-правовых последствиях действий лица, в отношении которого вынесен приговор суда, по вопросам, имели ли место эти действия и совершены ли они данным лицом.

Со стороны ответчика не представлено, а судом не добыто доказательств, подтверждающих, что **списание** денежных средств произведено в результате неправомерных действий банка.

Доказательств нарушения условий договора банком по использованию банковской **карты** также не представлено.

Довод ответчика о допущенных банком нарушениях правил безопасности опровергается материалами дела и противоречит нормам материального права.

Также несостоятелен довод о том, что денежные средства были переведены в счет пополнения баланса абонентов мобильных операторов сотовой связи, находящихся за пределами города Костромы, где в спорный период находилась Максимова В.В., поскольку не доказывает незаконность совершенных Банком операций по **списанию** денежных средств с **карты** ответчика.

При таких данных, с учетом вышеприведенных норм у Банка имелись основания полагать, что распоряжение о переводе денежных средств дано держателем **карты** в рамках установленных банковских правил посредством телефона, указанного им при подключении услуги "Мобильный банк", в связи с чем правовых оснований для приостановления операций в период в период с 26 октября по <дата>, равно как и возврата денежных средств на **карту** держателя у Банка не имелось, Банк действовал в соответствии с действующим законодательством Российской Федерации и заключенным с ответчиком договором, надлежащим образом выполнив свои обязательства по заключенному между сторонами договору. Нарушений Банком прав Максимовой В.В. как потребителя банковской услуги допущено не было, в связи с чем оснований для взыскания компенсации морального вреда не имеется.

Доводы ответчика основаны на неправильном толковании приведенных выше положений законодательства,

На основании вышеизложенного, руководствуясь ст.ст.194,198 ГПК РФ, суд

р е ш и л :

Исковые требования ПАО Сбербанк в лице филиала- Костромского отделения № удовлетворить.

Взыскать с Максимовой Виктории Владимировны в пользу ПАО Сбербанк в лице филиала- Костромского отделения № сумму задолженности по банковской **карте** № в размере 47851 рублей 86 коп., судебные расходы по оплате госпошлины в сумме 1635 руб. 56 коп.

В удовлетворении встречного иска Максимовой Виктории Владимировны к ПАО «Сбербанк России» о взыскании компенсации морального вреда отказать.

Решение может быть обжаловано сторонами в апелляционном порядке в течение месяца в Костромской областной суд через Свердловский районный суд г. Костромы.

Решение № 2-1094/2017 2-1094/2017~М-596/2017 М-596/2017 от 28 июня 2017 г. по делу № 2-1094/2017

Ярославский районный суд (Ярославская область) – Гражданское

Суть спора: 2.163 - О защите прав потребителей -> из договоров с финансово-кредитными учреждениями -> в сфере услуг кредитных организаций

Дело № 2-1094/17 Изг.ДД.ММ.ГГГГ.

РЕШЕНИЕ

ИМЕНЕМ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ярославский районный суд Ярославской области в составе:

председательствующего судьи Орловой Ю.В.,

при секретаре Волковой Р.А.,

рассмотрев в открытом судебном заседании в г. Ярославле 28 июня 2017 года гражданское дело по иску Пахомовой О.В. к АО «Альфа-Банк» о защите прав потребителей,

установил:

Пахомова О.В. обратилась в суд с иском к АО «Альфа-Банк», в котором указала, что ДД.ММ.ГГГГ. между нею и АО «Альфа-Банк» был заключен договор потребительского **кредита** №, предусматривающий выдачу **кредитной карты**, открытие и обслуживание счета **кредитной карты**. На основании указанного договора на имя истицы был открыт счет № в Банке и выдана **кредитная карта** № с **кредитным лимитом** <данные изъяты> рублей.

ДД.ММ.ГГГГ года впервые подключив Интернет-банк и зайдя в него, истица обнаружила, что ДД.ММ.ГГГГ года со счета указанной **кредитной карты списываются** денежные средства в размере <данные изъяты> руб. <данные изъяты> коп. Распоряжения на совершение указанной операции по счету **кредитной карты** истица Банку не давала. При этом, каких-либо уведомлений от Банка о совершении указанной операции, истица также не получала и не знала о ней до момента подключения Интернет-банка и входа в него ДД.ММ.ГГГГ года.

Узнав о **списании** денежных средств, истица незамедлительно ДД.ММ.ГГГГ года обратилась в Банк с письменным заявлением, в котором уведомила Банк о своем несогласии с обнаруженным **списанием** по счету **кредитной карты** и необходимости блокировки данной банковской операции. Одновременно истице была переоформлена сама **кредитная карта** с другим номером (выдан новый «пластик»), поскольку старая **кредитная карта** была заблокирована.

Несмотря на претензию истицы об оспаривании указанной операции и несогласии со **списанием** денежных средств, ДД.ММ.ГГГГ года со счета **кредитной карты** Банком

были необоснованно **списаны** денежные средства в размере <данные изъяты> руб. <данные изъяты> коп.

В этой связи ДД.ММ.ГГГГ года истицей было написано еще одно письменное заявление в Банк с указанием того, что истица не согласна с необоснованным **списанием** денежных средств (без распоряжения) и с требованием вернуть денежные средства на карточный счет.

До настоящего времени необоснованно **списанные** денежные средства в размере <данные изъяты> руб. <данные изъяты> коп. на банковский счет **кредитной карты** Банком не возвращены. Ответ на указанное заявление по существу вопроса на момент подачи настоящего иска от Банка не получен.

В соответствии с действующим законодательством, если Клиент уведомил Банк о **несанкционированном списании** денежных средств в указанный в законе срок, **списанная** в результате незаконной операции сумма возмещается оператором Банка.

В результате оказания услуги ненадлежащего качества истице были причинены убытки, и нанесен имущественный вред, выразившийся в том, что истица была вынуждена занимать денежные средства для их внесения на счет **кредитной карты** взамен необоснованно **списанной** с нее суммы в размере <данные изъяты> руб. <данные изъяты> коп. Вынужденный заем денежных средств повлек дополнительные материальные расходы в виде процентов от займа в размере <данные изъяты> руб. в месяц.

Кроме того, Банк ДД.ММ.ГГГГ. **списал** со счета **кредитной карты** комиссию за организацию страхования в размере <данные изъяты> руб. <данные изъяты> коп. Так как вышеуказанную операцию по счету **кредитной карты** истица не совершала и не давала Банку своего распоряжения на ее совершение, считает **списание** указанной суммы также неправомерным.

В результате некачественно оказанной ответчиком услуги истице был причинен моральный вред (постоянный стресс, душевные волнения, тяжелое душевное состояние и существенное ухудшение самочувствия). Для **восстановления** нормального физического и психологического состояния истица была вынуждена обратиться к соответствующим специалистам на платной основе, нести расходы на медицинские препараты.

ДД.ММ.ГГГГ года истицей в адрес ответчика была направлена претензия, которая на момент подачи иска в суд (ДД.ММ.ГГГГ.) не удовлетворена.

В целях получения квалифицированной юридической помощи истицей было заключено соглашение от ДД.ММ.ГГГГ. с адвокатом. Стоимость услуг по указанному соглашению составила <данные изъяты> рублей.

На основании изложенного, истица просит:

1. обязать ответчика вернуть на счет № **кредитной карты**:

- денежные средства в размере <данные изъяты> рублей <данные изъяты> коп., необоснованно **списанные** Банком со счета;

- денежные средства в размере <данные изъяты> руб. <данные изъяты> коп., необоснованно **списанные** Банком в качестве комиссии за организацию страхования.

2. взыскать денежные средства:

- убытки, связанные с необходимостью занимать денежные средства, чтобы пополнить счет **кредитной карты** в размере <данные изъяты> руб. и образовавшиеся в этой связи проценты в размере <данные изъяты> руб. за каждый месяц, всего за два месяца <данные изъяты> рубля;

- убытки в виде процентов на сумму необоснованного **списания** денежных средств в порядке и в размере, установленном ст.395 ГК РФ, с момента необоснованного **списания** по день возврата денежных средств на счет **кредитной карты** .

3. взыскать с ответчика штраф в размере 50% от суммы, присужденной судом в пользу потребителя.

4. взыскать с ответчика компенсацию морального вреда в размере <данные изъяты> рублей.

5. взыскать с ответчика расходы на оплату услуг представителя в размере <данные изъяты> рублей.

Пахомова О.В. в судебном заседании заявила отказ от исковых требований в части возврата на счет **карты** денежных средств в размере <данные изъяты> рублей <данные изъяты> коп., и денежных средств в размере <данные изъяты> руб. <данные изъяты> коп., поскольку данные денежные средства Банком были возвращены ДД.ММ.ГГГГ. В остальной части исковые требования поддержала.

Представитель истицы по устному ходатайству Соколов С.Н. в судебном заседании исковые требования поддержал.

От ответчика – АО «Альфа-Банк» поступил письменный отзыв, в котором указано, что денежные средства в размере <данные изъяты> руб. и <данные изъяты> руб. возвращены на счет клиента на основании рассмотренной претензии в добровольном порядке ДД.ММ.ГГГГ о чем истица была уведомлена СМС-сообщением, а также ответом, направленным ей по почте. Не признают исковые требования о взыскании процентов на указанные суммы за период с момента необоснованного **списания** по день возврата, поскольку указанные денежные средства истице никогда не принадлежали. Истица не может нести убытки в виде процентов за пользование чужими денежными средствами, поскольку эти денежные средства и для нее являются чужими. Истицей не представлено никаких доказательств, подтверждающих получение заемных денежных средств и трату их непосредственно на зачисление на свой счет. Кроме того, истицей принято решение о зачислении денежных средств на счет в таком размере по собственному усмотрению. Также не признают требования о компенсации морального вреда, поскольку истицей не представлено доказательств возникновения негативных последствий, а также причинная связь между имеющими место событиями и моральным вредом. Оснований для взыскания штрафа нет, поскольку требования истицы были удовлетворены банком добровольно.

Представитель третьего лица – Ярославского РОСП в судебное заседание не явился по неизвестному суду причине, о слушании дела извещен надлежаще.

Суд определил рассмотреть дело при имеющейся явке.

Выслушав истицу, ее представителя, проверив и исследовав письменные материалы дела, суд приходит к следующему

Согласно пункту 1 статьи 845 Гражданского кодекса Российской Федерации по договору банковского счета банк обязуется принимать и зачислять поступающие на счет, открытый клиенту (владельцу счета), денежные средства, выполнять распоряжения клиента о перечислении и выдаче соответствующих сумм со счета и проведении других операций по счету.

В соответствии со статьей 854 Гражданского кодекса Российской Федерации **списание** денежных средств со счета осуществляется банком на основании распоряжения клиента; без распоряжения клиента **списание** денежных средств, находящихся на счете, допускается по решению суда, а также в случаях, установленных законом или предусмотренных договором между банком и клиентом.

Договором может быть предусмотрено удостоверение прав распоряжения денежными суммами, находящимися на счете, электронными средствами платежа и другими документами с использованием в них аналогов собственноручной подписи (пункт 2 статьи 160), кодов, паролей и иных средств, подтверждающих, что распоряжение дано уполномоченным на это лицом (пункт 3 статьи 847 ГК РФ).

Согласно ст.1095 ГК РФ, вред, причиненный жизни, здоровью или имуществу гражданина либо имуществу юридического лица вследствие конструктивных, рецептурных или иных недостатков товара, работы или услуги, а также вследствие недостоверной или недостаточной информации о товаре (работе, услуге), подлежит возмещению продавцом или изготовителем товара, лицом, выполнившим работу или оказавшим услугу (исполнителем), независимо от их вины и от того, состоял потерпевший с ними в договорных отношениях или нет.

Из материалов дела видно, что ДД.ММ.ГГГГ. между Пахомовой О.В. и АО «Альфа-Банк» был заключен договор потребительского **кредита,** предусматривающий выдачу **кредитной карты,** открытие и **кредитование** Счета **Кредитной карты**.

Согласно Постановлению об отказе в возбуждении уголовного дела от ДД.ММ.ГГГГ., ДД.ММ.ГГГГ. в ОМВД России по Фрунзенскому району г. Ярославля поступило заявление от Пахомовой О.В. по факту **несанкционированного списания** денежных средств с банковской **карты** заявителя на общую сумму <данные изъяты> рублей. В ходе проведения проверки было установлено, что Пахомова О.В. в пользовании имеет **кредитную карту** ПАО «Альфа-Банк» с **кредитным лимитом** <данные изъяты> рублей. В Интернет-банк с указанной **карты** Пахомова О.В. не заходила до ДД.ММ.ГГГГ также не заходила в сеть Интернет со своего мобильного телефона. ДД.ММ.ГГГГ. Пахомова О.В. зашла Интернет банк, где обнаружила, что ДД.ММ.ГГГГ. с принадлежащей ей **кредитной карты** были **списаны** денежные средства в размере <данные изъяты> рублей.

Как следует из материалов дела, две претензии истицы в адрес АО «Альфа-Банк» от ДД.ММ.ГГГГ. и от ДД.ММ.ГГГГ. о возврате необоснованно **списанных** денежных средств на счет **карты** удовлетворены не были.

ДД.ММ.ГГГГ. Пахомовой О.В. была написана претензия, в которой истица просил вернуть на счет **кредитной карты** необоснованно **списанные** денежные средства, а также

возместить причиненные убытки, моральный вред и расходы за оказание юридической помощи.

Денежные средства в размере <данные изъяты> рублей и <данные изъяты> руб. <данные изъяты> коп. были зачислены на счет истицы ДД.ММ.ГГГГ года.

Таким образом, в ходе рассмотрения настоящего спора судом установлено, что распоряжения на выдачу спорных денежных средств истица не давала, что свидетельствует о некачественном оказании истице финансовой услуги, что в силу ч. 2 ст. 13 Федерального закона "О защите прав потребителей" является основанием для возмещения исполнителем убытков, причиненных потребителю.

Суд считает обоснованными исковые требования о взыскании процентов за пользование чужими денежными средствами, рассчитанными по правилам п.1 ст.395 ГК РФ, поскольку в указанный период времени истица по вине ответчика не имела возможности пользоваться денежными средствами.

Размер процентов за период с ДД.ММ.ГГГГ. по ДД.ММ.ГГГГ. будет составлять <данные изъяты> рублей <данные изъяты> копеек.

В силу пункта 2 Постановления Пленума Верховного Суда РФ от 28.06.2012г. N 17 "О рассмотрении судами гражданских дел по спорам о защите прав потребителей", если отдельные виды отношений с участием потребителей регулируются и специальными законами Российской Федерации, содержащими нормы гражданского права (например, договор участия в долевом строительстве, договор страхования, как личного, так и имущественного, договор банковского вклада, договор перевозки, договор энергоснабжения), то к отношениям, возникающим из таких договоров, Закон о защите прав потребителей применяется в части, не урегулированной специальными законами.

Согласно ст. 15 Закона РФ "О защите прав потребителей" моральный вред, причиненный потребителю вследствие нарушения изготовителем (исполнителем, продавцом, уполномоченной организацией или уполномоченным индивидуальным предпринимателем, импортером) прав потребителя, предусмотренных законами и правовыми актами Российской Федерации, регулирующими отношения в области защиты прав потребителей, подлежит компенсации причинителем вреда при наличии его вины. Размер компенсации морального вреда определяется судом и не зависит от размера возмещения имущественного вреда. Компенсация морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных потребителем убытков.

Фактом оказания некачественной финансовой услуги со стороны ответчика истице был причинен моральный вред, размер которого с учетом обстоятельств дела, индивидуальных особенностей истицы, суд определяет в <данные изъяты> рублей.

Исковые требования о взыскании заемных денежных средств в размере <данные изъяты> рублей и процентов в размере <данные изъяты> рублей удовлетворению не подлежат, поскольку материалами дела не подтверждается факт внесения указанных денежных средств на счет истицы; необходимость таких действий, в связи с чем, оснований считать указанные суммы убытками истицы, которые она понесла в связи с необоснованным **списанием** с ее счета денежных средств, у суда нет.

В силу п. 6 ст. 13 Закона РФ от 7.02.1992 года N 2300-1 "О защите прав потребителей", при удовлетворении судом требований потребителя, установленных законом, суд взыскивает с изготовителя (исполнителя, продавца, уполномоченной организации или уполномоченного индивидуального предпринимателя, импортера) за несоблюдение в добровольном порядке удовлетворения требований потребителя штраф в размере пятьдесят процентов от суммы, присужденной судом в пользу потребителя.

Из материалов дела следует, что сумма в размере <данные изъяты> руб. была возвращена истице после подачи иска в суд, в связи с чем, суд взыскивает с ответчика штраф в размере 50% от указанной суммы.

Согласно статье 100 ГПК РФ стороне, в пользу которой состоялось судебное решение, по ее письменному ходатайству суд присуждает с другой стороны расходы на оплату услуг представителя в разумных пределах.

Из материалов дела следует, что исковые требования судом удовлетворены частично, в связи с чем, Пахомова О.В. имеет право на возмещение судебных расходов.

При рассмотрении настоящего дела интересы Пахомовой О.В. представлял Соколов С.Н., которым были даны консультации по возникшему спору, составлена претензия, представитель принял участие в одном судебном заседании.

С учетом сложности спора (суд относит спор к категории средней сложности), объема проделанной представителем работы, требований разумности, суд определяет подлежащий возмещению размер расходов на оплату услуг представителя в <данные изъяты> рублей.

На основании изложенного и руководствуясь ст.ст.194-199 ГПК РФ, суд

решил:

Исковые требования удовлетворить частично.

Взыскать с АО «Альфа-Банк» в пользу Пахомовой О.В. проценты за пользование чужими денежными средствами в размере <данные изъяты> рублей, штраф в размере <данные изъяты> рублей, компенсацию морального вреда в размере <данные изъяты> рублей, расходы на оплату услуг представителя в размере <данные изъяты> рублей, а всего <данные изъяты> рубль.

Решение может быть обжаловано в Ярославский областной суд в течение месяца с момента изготовления решения суда в окончательной форме путем подачи жалобы в Ярославский районный суд Ярославской области.

Судья Ю.В.Орлова

Решение № 2-1128/2018 2-1128/2018 (2-12141/2017;) ~ М0-11429/2017 2-12141/2017 М0-11429/2017 от 8 февраля 2018 г. по делу № 2-1128/2018

Автозаводский районный суд г. Тольятти (Самарская область) - Гражданские и административные

ЗАОЧНОЕ

РЕШЕНИЕ

ИМЕНЕМ РОССИЙСКОЙ ФЕДЕРАЦИИ

08 февраля 2018 года г.Тольятти

Автозаводский районный суд г. Тольятти Самарской области в составе

председательствующего судьи Разумова А.В.,

при секретаре ФИО3,

рассмотрев в открытом судебном заседании гражданское дело № по иску ФИО2

ПАО «РОСБАНК» о защите прав потребителей,

УСТАНОВИЛ:

ФИО2 обратился в Автозаводский районный суд <адрес> с иском к ПАО «РОСБАНК» о защите прав потребителей и признании действий банка незаконными, в обоснование требований указав, что ДД.ММ.ГГГГ между истцом и ПАО «РОСБАНК» был заключен договор потребительского **кредитования** на сумму 55 000 руб.

04.08.2017г. истцом была получена **кредитная карта**.

06.08.2017г. на принадлежащий истцу номер телефона поступило СМС сообщение о **списании** с **карты** денежной суммы в размере 9 700 руб., с указание номера телефона горячей линии ВТБ-24. При обращении на телефон горячей линии, истцу сообщили о том, что возможно это ошибка и о возможности аннулирования трансакции, путем ввода цифр поступающих на мой номер телефона.

Разговаривая с «якобы сотрудником Банка», о чем истец узнал позже, ему на телефон поступали коды, которые он тут же ему сообщал для отмены **списания** суммы 9 700руб.

ДД.ММ.ГГГГ с целью проверить остаток на счете истец обратился в Росбанк за выпиской по счету, из которой увидел, что с открытой на его имя **кредитной карты** была **списана** денежная сумма в размере 50 280 руб., остаток на **карте** составил 4720 руб.

Истец сразу ДД.ММ.ГГГГ обратился в Банк с заявлением, в котором изложил факт неправомерного **списания** денежных средств с просьбой принять меры. Фактически, из существа поданного заявления истец просил Банк приостановить все операции по **карте** и разобраться в ситуации. Таким образом, ДД.ММ.ГГГГ Банк был извещен о том, что ПИН-код возможно стал известен третьему лицу, который завладел кодами обманным путем.

ДД.ММ.ГГГГ истцом также было написано заявление в полицию, на основании которого было возбуждено уголовное дело и истец признан потерпевшим.

Несмотря на данные обстоятельства Банк 08.08.2017г. и 09.08.2017г. проводит операции по счету и **списывает** с **кредитной карты**денежные суммы, якобы по поступившему от истца распоряжению ДД.ММ.ГГГГ, в общей сложности 50 280 руб.

Более того, на 06.08.2017г. на **кредитной карте** отсутствовали денежные средства, и только 08.08.2017г. на **карту** поступили **кредитные**деньги (что видно из выписки по счету), тогда как в Банке уже имелось заявление об отзыве/отмене операций.

В октябре 2017 г. истец вновь обратился в Банк с заявлением с описанием вышеизложенных обстоятельств и просил остановить начисление процентов до окончания следствия по возбужденному уголовному делу, на что получил отказ.

В данном случае, в день, а именно ДД.ММ.ГГГГ когда истцу стало известно о том, что ДД.ММ.ГГГГ от его лица даны распоряжения о**списании** денежных средств, непосредственно напрямую в письменном виде известил об этом Банк. Однако, не смотря на данное обстоятельство, ДД.ММ.ГГГГ Банк предоставляет истцу **кредит** на пополнение счета в размере 20 280 руб. и ДД.ММ.ГГГГ проводит две операции по переводу 6 880 руб. и 10 400 руб., далее ДД.ММ.ГГГГ предоставляет истцу **кредит** на пополнение счета в размере 30 000 руб. и ДД.ММ.ГГГГ проводит три операции по **списанию** сумм по 10 000 руб.

Данные действия Банка истец считает незаконными, поскольку при надлежащим уведомлении Банка еще ДД.ММ.ГГГГ о совершении в отношении истца мошеннических действий, в последующие два дня Банком производятся операции, несмотря на тот факт, что в момент извещения Банка ДД.ММ.ГГГГ безотзывность перевода денежных средств не наступила.

Более того, в момент проведения операций по **списанию** денежных средств на телефон истцу не приходили извещения Банка о проводимых операциях и их суммах.

На основании вышеизложенного, истец просит признать действия ПАО «РОСБАНК» по проведению операций по счету 40№, принадлежащему ФИО2, по **списанию** денежных средств по документу № от ДД.ММ.ГГГГ на сумму 9880 руб., по документу № от ДД.ММ.ГГГГ на сумму 10 400 руб., по документу № от ДД.ММ.ГГГГ, по документу № на сумму 10 000 руб., по документу № на сумму 10 000 руб. - незаконными. Обязать ПАО «РОСБАНК» **восстановить** положение, существовавшее до нарушения прав ФИО2, путем **восстановления** суммы **лимита кредитной карты** №.

В судебном заседании представитель истца ФИО4, действующая по доверенности, требования, изложенные в иске, поддержала, просила иск удовлетворить в полном объеме.

Представитель ответчика в судебное заседание не явился, о времени и месте судебного заседания извещен надлежащим образом, причину неявки суду не сообщил, ранее направил отзыв, согласно которому требования истца основаны на неверном толковании норм права и не подлежат удовлетворению, поскольку, спорные операции по переводу денежных средств осуществлены на основании распоряжения клиента, путем использования одноразового пароля, направленного банком на номер мобильного телефона истца. При этом, в обязанность клиента в соответствии с п.5.10. условий входит не разглашать одноразовый пароль никаким третьим лицам. Риск проведенных транзакций при сообщении одноразового пароля третьим лицам несет клиент.

Суд, выслушав пояснения представителя истца, изучив письменные материалы гражданского дела, оценивая собранные доказательства по своему внутреннему убеждению, основанному на всестороннем, полном, объективном и непосредственном исследовании каждого доказательства в отдельности, а также в их совокупности, находит иск обоснованным и подлежащим удовлетворению по следующим основаниям.

В соответствии со ст. 854 ГК РФ **списание** денежных средств со счета осуществляется банком на основании распоряжения клиента. Без распоряжения

клиента **списание** денежных средств, находящихся на счете, допускается по решению суда, а также в случаях, установленных законом или предусмотренных договором между банком и клиентом.

В силу ст. 856 ГК РФ в случаях несвоевременного зачисления на счет поступивших клиенту денежных средств либо их необоснованного**списания** банком со счета, а также невыполнения указаний клиента о перечислении денежных средств со счета либо об их выдаче со счета банк обязан уплатить на эту сумму проценты в порядке и в размере, предусмотренных статьей 395 настоящего Кодекса.

Согласно ч. 3 ст. 864 ГК РФ поручение плательщика исполняется банком при наличии средств на счете плательщика, если иное не предусмотрено договором между плательщиком и банком.

В силу ч. 3 ст. 865 ГК РФ банк обязан незамедлительно информировать плательщика по его требованию об исполнении поручения. Порядок оформления и требования к содержанию извещения об исполнении поручения предусматриваются законом, установленными в соответствии с ним банковскими правилами или соглашением сторон.

Таким образом, по общему правилу, **списание** денежных средств со счета осуществляется банком на основании распоряжения клиента. Без распоряжения клиента **списание** денежных средств, находящихся на счете, допускается по решению суда, а также в случаях, установленных законом или предусмотренных договором между банком и клиентом.

В судебном заседании установлено и сторонами не оспаривается, что ДД.ММ.ГГГГ между истцом и ПАО «РОСБАНК» был заключен договор потребительского **кредитования,** на сумму 55 000 руб.

ДД.ММ.ГГГГ истцом была подучена **кредитная карта,** что подтверждается индивидуальными условиями договора потребительского**кредита** с **лимитом кредитования** (**кредитная карта**), заявлением об открытии счета по **карте** и предоставлении **карты** , копии которых приложены в материалы дела (л.д.6-10).

ДД.ММ.ГГГГ на принадлежащий истцу номер телефона поступило СМС сообщение о **списании** с **карты** денежной суммы в размере 9 700 руб., с указание номера телефона горячей линии ВТБ-24. При обращении на телефон горячей линии, истцу сообщили о том, что возможно это ошибка и о возможности аннулирования трансакции, путем ввода цифр, поступающих на номер телефона истца.

ДД.ММ.ГГГГ с целью проверить остаток на счете истец обратился в Росбанк за выпиской по счету, из которой увидел, что с открытой на его имя **кредитной карты** была **списана** денежная сумма в размере 50 280 руб., остаток на **карте** составил 4720 руб., что подтверждается выпиской по счету, копия которого приложена к материалам дела (л.д.12).

ДД.ММ.ГГГГ истцом в адрес ответчика было направлено заявление, в котором истец просил прекратить все операции по **карте** , поскольку ПИН-код возможно стал известен третьему лицу (л.д. 13-15).

ДД.ММ.ГГГГ истец обратился в правоохранительные органы, о чем свидетельствует талон-уведомление №, копия которого представлена в материалы дела (л.д.19).

Постановлением от ДД.ММ.ГГГГ старшим следователем отдела по расследованию преступлений, совершенных на территории <адрес> СУ УМВД России по <адрес> было возбуждено уголовное дело, по признакам преступления, предусмотренного ч.2 ст.159 УК РФ, копия постановления приложена к материалам дела (л.д.20).

Постановлением от ДД.ММ.ГГГГ истец был признан потерпевшим (л.д.22).

Как следует из представленной в материалы дела выписки по лицевому счету от ДД.ММ.ГГГГ с **карты** истца в период с ДД.ММ.ГГГГ по ДД.ММ.ГГГГ проводятся операции по **списанию** денежных средств на общую сумму 50280 руб. (л.д.11).

ФЗ №161-ФЗ «О национальной платежной системе» устанавливает правовые и организационные основы национальной платежной системы, регулирует порядок оказания платежных услуг, в том числе осуществления перевода денежных средств, использования электронных средств платежа (ст.1).

В соответствии с п. 1 ст. 5 указанного Закона оператор по переводу денежных средств осуществляет перевод денежных средств по распоряжению клиента (плательщика или получателя средств), оформленному в рамках применяемой формы безналичных расчетов (далее - распоряжение клиента). Перевод электронных денежных средств осуществляется на основании распоряжений плательщиков в пользу получателей средств (п. 7 ст. 7 Закона).

В соответствии со ст. 7 Федерального закона от 27.06.2011 N 161-ФЗ "О национальной платежной системе":

Частью 10 указанного закона перевод электронных денежных средств осуществляется путем одновременного принятия оператором электронных денежных средств распоряжения клиента, уменьшения им остатка электронных денежных средств плательщика и увеличения им остатка электронных денежных средств получателя средств на сумму перевода электронных денежных средств либо в срок, предусмотренный частью 11 настоящей статьи.

Перевод электронных денежных средств с использованием предоплаченной **карты** осуществляется в срок не более трех рабочих дней после принятия оператором электронных денежных средств распоряжения клиента, если более короткий срок не предусмотрен договором, заключенным оператором электронных денежных средств с клиентом, либо правилами платежной системы.

Договором, заключенным оператором электронных денежных средств с клиентом, может быть предусмотрена возможность использования плательщиком - физическим лицом и получателем средств - юридическим лицом или индивидуальным предпринимателем электронных средств платежа, когда действия, указанные в части 10 настоящей статьи, осуществляются неодновременно (далее - автономный режим использования электронного средства платежа). В таком случае получатель средств обязан ежедневно передавать информацию о совершенных операциях оператору электронных денежных средств для ее учета не позднее окончания рабочего дня оператора электронных денежных средств. Настоящая часть распространяется на переводы электронных денежных

средств с использованием доплаченной **карты,** если иное не предусмотрено договором, заключенным оператором электронных денежных средств с получателем средств или с оператором по переводу денежных средств, либо правилами платежной системы.

Оператор электронных денежных средств незамедлительно после исполнения распоряжения клиента об осуществлении перевода электронных денежных средств направляет клиенту подтверждение об исполнении указанного распоряжения.

В случае автономного режима использования электронного средства платежа оператор электронных денежных средств направляет плательщику и в случае, предусмотренном договором, получателю средств подтверждения об осуществлении перевода электронных денежных средств незамедлительно после учета оператором электронных денежных средств информации, полученной в соответствии с частью 12 настоящей статьи. Настоящая часть распространяется на переводы электронных денежных средств с использованием предоплаченной **карты** , если иное не предусмотрено договором, заключенным оператором электронных денежных средств с получателем средств или с оператором по переводу денежных средств, либо правилами платежной системы.

Перевод электронных денежных средств становится безотзывным и окончательным после осуществления оператором электронных денежных средств действий, указанных в части 10 или 11 настоящей статьи.

Часть 9 ст. 8 Федерального закона от 27.06.2011 N 161-ФЗ "О национальной платежной системе" (далее - Закон N 161-ФЗ) закрепляет право клиента отозвать свое распоряжение о переводе денежных средств до наступления безотзывности перевода в порядке, установленном законодательством и договором с оператором электронных денежных средств. Аналогичное правило содержится и в Положении о правилах осуществления перевода денежных средств, утвержденном Банком России 19.06.2012 N 383-П (далее - Положение N 383-П), в п. 2.14 которого отзыв распоряжения клиента осуществляется до наступления безотзывности перевода денежных средств.

Отзыв распоряжения о переводе денежных средств по банковскому счету осуществляется на основании заявления отправителя распоряжения об отзыве, которое представляется в электронном виде или на бумажном носителе в банк.

Банк не позднее рабочего дня, следующего за днем поступления заявления об отзыве, направляет отправителю распоряжения уведомление в электронном виде или на бумажном носителе об отзыве. В этом уведомлении указывается дата, возможность (невозможность в связи с наступлением безотзывности перевода денежных средств) отзыва распоряжения.

В памятке Центрального Банка России от ДД.ММ.ГГГГ "О мерах безопасности использования банковских **карт**", указывается на то, что в случае раскрытия ПИН, персональных данных, утраты банковской **карты** существует риск совершения неправомерных действий с денежными средствами на банковском счете со стороны третьих лиц.

До момента обращения в **кредитную** организацию – эмитент банковской **карты** несет риск, связанный с **несанкционированнымсписанием** денежных средств с банковского счета.

В соответствии с п.2 заявления об открытии счета по **карте** и предоставлении **кредитной карты** , клиент знает и согласен с тем. что в случае утери или кражы **карты** , в случае если клиент узнал, что Пины стали известны другому лицу, а также в иных случаях обнаружения клиентом факта использования **Карты** без его согласия, для приостановки операций по СПК. совершаемых с использованием **Карты** , я обязан незамедлительно сообщить об этом в Контакт-центр Банка по телефону, но не позднее дня. следующего за днем информирования Банком Клиента об операции, которая была совершена без его согласия.

Между тем, материалами дела установлено и сторонами не оспаривается, что истец ДД.ММ.ГГГГ обратился к ответчику с письменным заявлением, в котором указал о наличии мошеннических действий со стороны третьих лиц, которые повлекли за собой **списание** денежных средств со счета истца.

В соответствии с п. п. 10, 15 ст. 7 Федерального закона от 27.06.2011 N 161-ФЗ "О национальной платежной системе", безотзывность перевода электронных денежных средств наступает после осуществления оператором электронных денежных средств одновременного принятия распоряжения клиента, уменьшения остатка электронных денежных средств плательщика и увеличения остатка электронных денежных средств получателя средств на сумму перевода электронных денежных средств.

Клиент вправе отозвать свое распоряжение о переводе денежных средств до наступления безотзывности перевода в порядке, установленном законодательством и договором с оператором электронных денежных средств; если иное не обусловлено применяемой формой безналичных расчетов или федеральным законом, безотзывность перевода денежных средств наступает либо с момента**списания** денежных средств с банковского счета плательщика, либо с момента предоставления плательщиком наличных денежных средств в целях перевода денежных средств без открытия банковского счета; безотзывность перевода электронных денежных средств наступает после осуществления оператором электронных денежных средств одновременного принятия распоряжения клиента, уменьшения остатка электронных денежных средств плательщика и увеличения остатка электронных денежных средств получателя средств на сумму перевода электронных денежных средств. Допускается также автономный режим использования электронного средства платежа, который может быть предусмотрен договором между оператором электронных денежных средств и клиентом; автономный режим использования электронного средства платежа означает, что перечисленные выше действия оператора электронных денежных средств будут осуществляться не одновременно; в случае автономного режима использования электронного средства платежа перевод электронных денежных средств становится безотзывным в момент использования клиентом электронного средства платежа. Отзывраспоряжения о переводе денежных средств по банковскому счету осуществляется на основании заявления отправителя распоряжения об отзыве, которое представляется в электронном виде или на бумажном носителе в банк; банк не позднее рабочего дня, следующего за днем поступления заявления об отзыве, направляет отправителю распоряжения уведомление в электронном виде или на бумажном носителе об отзыве; отзыв распоряжения, переданного с использованием электронного средства платежа, осуществляется клиентом посредством отмены операции с использованием

электронного средства платежа. Распоряжение клиента о переводе денежных средств может быть им отозвано до наступления безотзывности перевода денежных средств.

Таким образом, судом установлено, что банк получил прямое распоряжение истца об отмене операции (ДД.ММ.ГГГГ). Данное распоряжение было получено банком до наступления периода безотзывности, который наступает с момента **списания** денежных средств клиента, то есть ДД.ММ.ГГГГ

Каких-либо доказательств, свидетельствующих о наступлении периода безотзывности ранее даты, в которую истцом было направлено в адрес банка распоряжение об отмене операций, а именно ранее ДД.ММ.ГГГГ ответчиком в материалы дела не представлено.

На основании вышеизложенного, суд приходит к выводу о том, что истец, воспользовался своим правом по отзыву распоряжения о переводе денежных средств до момента наступления периода безотзывности, факт получения распоряжения стороной ответчика в судебном заседании не оспаривался.

Ответчиком данное распоряжение исполнено не было, действия банка по проведению операций по счету истца после получения распоряжения являются незаконными.

Таким образом, поскольку, суд признал действия ответчика в части проведения операций по счету, принадлежащему ФИО5 – незаконными, в судебном заседании было установлено, и сторонами не оспаривалось, что со счета истца были **списаны** денежные средства ДД.ММ.ГГГГ на общую сумму 50280 руб., чем были нарушены права ФИО2 как держателя **карты** , требования истца об обязании ответчика о **восстановлении** положения, существовавшего до нарушения прав ФИО2 путем **восстановления** суммы **лимита кредитной карты** суд находит обоснованными и подлежащими удовлетворению.

Принимая во внимание изложенное, руководствуясь ст. ст. 194-199 ГПК РФ, суд

РЕШИЛ:

Исковые требования ФИО2 к ПАО «РОСБАНК» о защите прав потребителей– удовлетворить.

Признать действия ПАО «РОСБАНК» по проведению операций по счету 40№, принадлежащему ФИО2., по **списанию** денежных средств по документу № от ДД.ММ.ГГГГ на сумму 9880 руб., по документу № от ДД.ММ.ГГГГ на сумму 10 400 руб., по документу № от ДД.ММ.ГГГГ, по документу № на сумму 10 000 руб., по документу № на сумму 10 000 руб. - незаконными.

Обязать ПАО «РОСБАНК» **восстановить** положение, существовавшее до нарушения прав ФИО2, путем **восстановления** суммы **лимита кредитной карты** № на имя ФИО2.

Ответчик вправе подать в суд, принявший заочное решение, заявление об отмене этого решения суда в течение семи дней со дня вручения ему копии этого решения.

Заочное решение суда может быть обжаловано сторонами также в апелляционном порядке в течение месяца по истечении срока подачи ответчиком заявления об отмене этого

решения суда, а в случае, если такое заявление подано - в течение месяца со дня вынесения определения суда об отказе в удовлетворении этого заявления. Решение в окончательной форме изготовлено 13.02.2018 года. Судья А.В. Разумов

5.4. Материалы экспертов о развитии законодательства

5.4.1. Различные мнения и комментарии об изменениях и дополнениях в закон "О национальной платежной системе".

- **Царьград – Банкам дали законное право на блокировку карт: Последствия для потребителей https://tsargrad.tv/articles/bankam-dali-zakonnoe-pravo-na-blokirovku-kart-posledstvija-dlja-potrebitelej_137207**

«Российские банки получили право блокировать сомнительные дистанционные операции своих клиентов. Соответствующий законопроект прошел третье чтение в Государственной Думе.

Документ, нацеленный на предотвращение хищения денежных средств с банковских карт, легализует уже существующую практику блокировки подозрительных операций кредитными организациями и устанавливает правила игры на этом поле.

Правда, эксперты подчеркивают, что вместе с правом по приостановке операций российские банки обрели обязанность отслеживать сомнительные транзакции. И профучастникам рынка очевидно, что эту обязанность придется исправно выполнять.

Согласно принятым депутатами законопроекту, банк сможет приостанавливать перевод на срок до 2 рабочих дней, если у кредитной организации появились подозрения, что операция прошла без согласия владельца счета. В случае подозрительных операций по счетам юридических лиц, у банка есть 5 рабочих дней на приостановку транзакций.

Помимо этого банки получают возможность блокировки электронных кошельков, мобильных приложений и предоплаченных банковских карт. При этом банк должен будет проинформировать клиента о своих подозрениях, чтобы тот имел возможность подтвердить правомерность операции или заявить о краже.

Кроме того, если по физическим лицам механизм возврата средств уже проработан, и этот процесс ограничен 30 днями, то ситуацию с юридическими лицами регламентирует как раз новое законодательство. Документ предлагает упрощенный механизм досудебного возврата средств в случае проблемных транзакций юрлица и тем самым восполняет пробел в законодательстве.

Отметим, что дать право банкам блокировать все сомнительные операции и переводы без предупреждения клиентов Минфин предложил еще в 2017 году, и в начале 2018 года соответствующие поправки в закон о Национальной платежной системе (НПС) прошли первое чтение в Госдуме.

Основанием для появления поправок стало два взаимосвязанных фактора: рост количества несанкционированных операций – в 2016 году было совершено порядка 300 тыс. операций с картами на сумму свыше 1 млрд рублей – и «отсебятина» со стороны

банковского сообщества, вызванная отсутствием четкого регламента действий в случае подозрений на незаконные транзакции.

При этом Банк России прогнозирует в 2018 году дальнейший рост количества криминальных операций, в том числе в секторе дистанционного банковского обслуживания (ДБО).

Криминал был, не было закона

Сталкиваясь с подозрительными транзакциями, российские банки довольно часто принимали решение по блокировке карты в отсутствии права по приостановке транзакций в секторе ДБУ.

Как отметил директор по мониторингу электронного бизнеса Альфа-Банка Алексей Голенищев, право блокировать карту клиента у банка есть и сейчас, поскольку она является собственностью банка. «А вот право приостанавливать транзакции для сервисов дистанционного банковского обслуживания, как интернет-банк, мобильный банк, переводы – это, действительно, необходимая практика», – цитируем эксперта по ТАСС.

До принятия поправок единого законодательного правила в этой сфере не было, и сектор контроля за правомерностью транзакций был отдан на откуп самих банков. Кредитные учреждения сами составляли собственный регламент управления рисками, где предусматривали подобные вещи, отметил в беседе с «Царьградом» аналитик ГК «Финам» Алексей Коренев.

Остановите афериста: Чубайс решил «присвоить» деньги будущих пенсионеров

«Если банк видел, что операция по тем или иным счетам носит признак криминальной или подозрительной, кредитная организация связывалась с клиентом и уточняла, действительно ли клиент совершал операцию, или платеж исполняется без его ведома, – рассказал аналитик. – Это касалось не только снятия денег с помощью банковской карты, но и зачисления больших сумм от физлица на физлицо».

По его словам, подобные действия банки совершали исключительно по собственной инициативе. Зато теперь отслеживание криминальных транзакций и их блокировка приобретает обязательный порядок, подчеркнул эксперт.

Кто тут подозрительный?

При этом "вишенкой на торте" принятых поправок являются критерии отнесения транзакций к подозрительным, которые должен в самое ближайшее время представить Банк России.

Профучастники рынка волнуются: не станут ли признаки основанием для блокировок «хороших» операций, и не приведет ли данная мера к выходу клиентов в наличность?

Опасения высказывают и представители малого бизнеса. По их словам, при осуществлении своей деятельности бизнес выполняет большое количество переводов, которые банк может счесть подозрительными. Кроме того, с 1 июля предприниматели переходят на «онлайн-кассы», а это означает что количество «подозрительных» операций может вырасти в разы.

Закон вступает в силу спустя 90 дней после опубликования, рассказывает А.Коренев. По его словам, до этого момента банки должны успеть привести в соответствие с новыми требованиями ЦБ свои внутренние регламенты. «Я думаю, что признаки появятся в самое ближайшее время», – сказал эксперт, указав, что банковские регламенты – дело небыстрое.

"Мы ждем пояснений от Центробанка, где будет, во-первых, указан полный перечень подозрительных транзакций или их признаков, а во-вторых, обозначены механизмы пользования единой базой данных. Следующего хода мы ждем от Банка России", - заключил А.Коренев.

Добровольно-принудительный порядок

Комментируя новый закон, эксперты подчеркивают: с его появлением контроль за операциями в сфере дистанционного банковского обслуживания переходит на государственный уровень.

«Документ закрепляет право банка приостанавливать подозрительные операции, но если вчитаться, он является обязательным для кредитных учреждений, подчеркнул А.Коренев. – То есть все же, речь идет не о праве, а об обязанности мониторить операции клиентов на предмет выявления подозрительных действий».

При этом у российских банков был инструмент по блокировке подозрительных счетов на законных основаниях. Речь идет о ФЗ-115 "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма". Не создают ли "блокировочные" законы избыточное регулирование?

По словам А.Коренева, ФЗ-115 имеет более широкий периметр действия, и касается не только транзакций по банковским картам, но и распространяется на все прочие операции в финансовой сфере. «Под действие этого закона чаще всего подпадают брокерские операции, когда выявляются сделки, подозрительные с точки зрения экономической целесообразности, то есть «отмывание» средств, незаконный вывод активов и так далее», – рассказал он.

Если в рамках 115-го закона отслеживались только крупные операции, то новый документ распространяется на более частные случаи, подчеркнул эксперт.

«Я не думаю, что со вступлением поправок в силу что-то усложнится, просто одно из направлений борьбы с криминалом, касающееся операций с дистанционным обслуживанием, будет более четко регламентировано», – заключил А.Коренев.

Ремень безопасности

Несмотря на отсутствие информации о сути поправок, а именно перечня операций, которые Банк России счел бы подозрительными, эксперты позитивно оценивают законопроект.

«Это сделано однозначно в интересах банковских клиентов, – сказал А.Коренев. – Конечно, многие потребители услуг кредитных организаций будут ворчать, что у них в самый ответственный момент заблокировали перевод за границей, и так далее. Мы так устроены, что пока у нас деньги не украли, нас раздражает излишний контроль. При этом, при пропаже средств клиент хватается за голову и думает: уж лучше бы меня 20 раз побеспокоили».

По его словам, «это из разряда таких вещей как мотоциклетный шлем или ремень безопасности в автомобиле». Эти средства мешают, но в конечном итоге, когда-нибудь могут спасти, отметил аналитик.

Тем не менее, рассчитывать на скорое решение проблем с кражей банковских средств не стоит. Какими бы прогрессивными ни были критерии для блокировки транзакций, все предусмотреть невозможно, считают эксперты. Всегда найдутся лазейки, которые злоумышленники найдут, чтобы эти критерии обойти.

Перечень Банка России будет дорабатываться, да и платежные системы не стоят на месте, рассуждают эксперты. Будут совершенствоваться технологии оплаты, будут модернизироваться и регламенты по выявлению незаконных операций, но добиться полной победы все равно не просто.

Как всегда, это будет вечная борьба мошенников с регулятором, и эффективность подобных запретов носит временный характер. Все заинтересованные стороны беспрерывно совершенствуются и стимулируют прогресс друг друга, подчеркнули эксперты».

- **РБК – ЦБ назвал признаки сомнительных операций для блокировки**
  https://www.rbc.ru/finances/28/09/2018/5bae2eba9a7947588831bc20

«ЦБ опубликовал признаки операций, которые банкам следует блокировать. Среди них операции с нетипичными для владельца счета параметрами

Банк России опубликовал список признаков несанкционированных операций, которые банки должны блокировать из-за возможного отсутствия согласия на них клиентов. Документ направлен на противодействие несанкционированным операциям и защиту клиентов от хищения средств кибермошенниками, говорится в сообщении регулятора.

Федеральный закон 167-ФЗ, позволяющий банку на два дня блокировать карты и денежные переводы со счетов клиентов, если возникнет подозрение в отношении операции, вступил в силу два дня назад. Теперь ЦБ дал разъяснения, что это за операции.

«Социальные инженеры»: как не попасться в ловушку кибермошенников

ДЕНЬГИ

Регулятор указал всего три признака операций, которые могут проводиться без ведома владельца счета для кражи его денег. В первую очередь банк должен приостановить денежный перевод, если информация о его получателе уже есть в базе данных ЦБ о случаях и попытках хищений. Второй признак несанкционированнной операции – совпадение параметров устройств, используемых для перевода через информационную систему, например интернет-банка, с информацией из той же базы данных ЦБ. Третий признак – несоответствие характера, объема, а также параметров совершаемых операций тем, которые обычно проводит клиент: время, день и место транзакции или использованные для этого устройства. Операция может также рассматриваться как потенциально несанкционированная, если обычной деятельности клиента не соответствуют ее сумма и периодичность.

Регулятор не прописывает, как банкам выявлять такие транзакции. Все операторы платежей решают сами, как проверять подлинность операций в рамках систем управления рисками. Если банк сочтет, что операция содержит признаки несанкционированной, он должен незамедлительно связаться с клиентом для выяснения, знает ли тот о проведении транзакции Если связаться не удалось, банк вправе приостановить такую операцию на срок до двух суток.

В середине 2018 года в законе «О национальной платежной системе» была закреплена обязанность ЦБ вести базу данных о попытках несанкционированных операций на основании предоставляемой ему банками информации, отмечает ведущий методолог «Эксперт РА» Юрий Беликов. «Видимо, база данных достаточно наполнилась, и процесс теперь можно сделать двусторонним: в онлайн-режиме поставлять банкам информацию из базы данных, чтобы они могли оперативно идентифицировать и блокировать несанкционированные операции, что немного сократит их издержки», – говорит он.

Повальной приостановки операций не будет: банки уже давно блокируют сомнительные операции клиентов, в том числе имеющие признаки несанкционированных, добавляет эксперт. «Как правило, проблема решается одним звонком сотрудников финмониторинга банка клиенту», – говорит Беликов».

- **Коммерсант – Банкам и клиентам придется договориться**
  https://www.kommersant.ru/doc/3841587

«ЦБ оставил рынок без рекомендаций по приостановке операций

Банкирам не удалось добиться от ЦБ разъяснений по спорным моментам недавно появившейся у них обязанности остановки подозрительных операций до получения согласия клиента. Регулятор оставил порядок информирования, запроса клиента и форму ответа, а также иные моменты на усмотрение банков, предоставив урегулировать все нюансы договором. По мнению юристов, такая вольность чревата возникновением множества спорных ситуаций, которые в итоге придется урегулировать в суде, что добавит проблем и банкам, и клиентам.

Ассоциация банков России (АБР) опубликовала ответ ЦБ на вопросы, касающиеся их обязанности останавливать трансакции клиентов при подозрениях в их несанкционированном характере. Такая обязанность возникла в связи с поправками к закону «О национальной платежной системе», которые вступили в силу 26 сентября 2018 года. Однако формулировки в законе оказались весьма неконкретными, допускающими двоякое толкование. В итоге банки написали ЦБ письмо со списком из более 40 вопросов с просьбой дать разъяснения, в отдельных случаях даже просили урегулировать порядок действий на уровне нормативного акта. Но Банк России, по сути, уклонился от ответа, напомнив о свободе договора банка с клиентом или просто процитировав нормы закона.

В результате открытыми остались вопросы взаимодействия банка–отправителя денежных средств и клиента в случаях выявления кредитной организацией сомнительной операции. В частности, по закону при выявлении попытки хищения клиентских средств банк обязан приостановить операцию на два дня, незамедлительно уведомить клиента об этом и после получения подтверждения провести трансакцию (или не проводить). Но как именно информировать клиента и в какой форме должно быть получено его согласие или отказ от проведения операции, закон не разъясняет, а вариантов много.

В ситуации взаимодействия банка–получателя средств и клиента проблемы еще серьезнее. Банк-получатель может задержать сомнительные средства на счете на пять дней, в течение которых клиент должен предъявить подтверждающие легальность денег документы. О каких именно документах идет речь и в каком виде их нужно представить, закон не разъясняет, не говоря уже о том, как проверить подлинность представленных документов.

Получить ответы банкиры надеялись от ЦБ. «Формулировки закона весьма неоднозначны, вопросы по трактовке тех или иных положений возникают постоянно», – отмечает директор управления информационной безопасности ОТП-банка Сергей Чернокозинский. «Жесткого регламентирования нормативным актом ЦБ отношений банка и клиента в сфере применения закона 167-ФЗ не нужно, так как сложно предусмотреть все ситуации, – уверен глава совета АБР Анатолий Аксаков. – В то же время по сложным моментам необходимы разъяснительные письма ЦБ с рекомендациями, которые очень помогут рынку».

Уверены в необходимости более четкого регулирования и юристы. «Проблема в том, что по ряду вопросов ЦБ просто не дает разъяснений, – отмечает управляющий партнер УК "Право и бизнес" Александр Пахомов. – Например, как быть, если клиент сначала сам подтвердил операцию, а после назвал ее хищением?» При отсутствии четкой позиции ЦБ банки могут действовать по-разному в одной ситуации, что недопустимо, указывает эксперт.

Банк России принимает на себя ключевую роль в вопросах антифрода, но при этом вопросы оформления взаимодействия банков и клиентов оставляет на усмотрение сторон, рассуждает партнер юридического бюро «Замоскворечье» Дмитрий Шевченко. По мнению эксперта, это несет серьезные риски. «Например, банк в договоре пропишет устную форму подтверждения клиента на проведение операции, и в случае хищения недобросовестный банк может сказать: клиент операцию подтвердил, а значит, банк ни за что не отвечает, даже если это было в действительности не так, – отмечает он.– Банк России должен дать по этому поводу более емкие рекомендации».

Если ЦБ не установит четкие регуляторные правила, то велик риск, что и в договоре банки не пропишут все нюансы, отмечает глава коллегии адвокатов «Старинский, Корчаго и партнеры» Евгений Корчаго. И тогда, предостерегает он, уже судам «по-живому» нужно будет устанавливать нормы и правила для взаимодействия банка и клиента в рамках 167-ФЗ».

5.4.2. Комментарии о дополнениях в закон "О потребительском кредите (займе)"

Федеральный закон от 07.03.2018 N 53-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации" (статья 4) дополнил статью 10 федерального закона "О потребительском кредите (займе)" положениями об обязанности кредитора «после совершения заемщиком каждой операции с использованием электронного средства платежа, с использованием которого заемщику был предоставлен потребительский кредит (заем), проинформировать заемщика о размере его текущей задолженности перед кредитором по договору потребительского кредита (займа) и о доступной сумме потребительского кредита (займа) с лимитом кредитования по договору потребительского

кредита (займа) путем включения такой информации в уведомление, предусмотренное частью 4 статьи 9 Федерального закона от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе".

- **РБК – Банки начнут информировать клиентов о задолженности после каждой операции**
  https://www.rbc.ru/finances/21/02/2018/5a8c38f19a79470a441aea4a

«Новые поправки в законодательство обязывают банки сообщать клиенту о размере его задолженности после каждой операции по кредитной карте. Это будет препятствовать росту просрочки, но увеличит издержки кредиторов, говорят эксперты.

Кредиторы должны будут информировать заемщика о задолженности и об остатке лимита по договору потребительского кредита (займа) после каждой операции клиента с использованием платежных карт. Соответствующие поправки в понедельник, 19 февраля, внесены ко второму чтению в федеральный закон №353-ФЗ «О потребительском кредите (займе)».

На текущий момент такая обязанность законодательно не закреплена за кредиторами. Новая мера направлена на улучшение информирования клиентов о совершении каждой операции с использованием платежных карт, следует из пояснительной записки к законопроекту. Конкретизация данных об имеющейся задолженности и остатке лимита кредитования позволит исключить заблуждение клиента, говорится в документе.

Глава комитета Госдумы по финансовому рынку Анатолий Аксаков пояснил РБК, что сейчас лишь отдельные банки полноценно информируют клиентов о размере кредитной задолженности. В связи с этим россияне нередко воспринимают сведения об остатках на карте как собственные, а не кредитные средства, пояснил он.

Кредитки – драйвер роста

Как ранее писал РБК, в 2017 году общая сумма выданных россиянам кредитов выросла на 37%, до 5,68 трлн руб. Лидером по темпам роста стал сегмент кредитных карт, заявили в Объединенном кредитном бюро. Число кредитных карт выросло на 8%, объемы одобренных лимитов – на 48%, сумма среднего лимита по карте – с 46 тыс. до 63 тыс. руб. Эксперты отмечают, что россияне все чаще берут кредиты для рефинансирования уже имеющихся. В Центральном банке уже начали принимать меры по оперативному реагированию на перегрев на рынке кредитования. Как писал РБК, регулятор готовит поправки, которые позволят изменять коэффициенты риска для отдельных сегментов банковского сектора решением совета директоров.

Что клиенты знают о долге

В соответствии с законом «О национальной платежной системе» каждый банк обязан уведомлять клиентов о совершении каждой операции по картам. Как правило, банки в своих СМС-сообщениях предоставляют информацию о балансе, то есть о сумме доступных для расходования средств.

РБК опросил топ-30 банков о том, как именно они информируют клиентов о размере задолженности по кредитным и овердрафтным картам. Из восьми банков, ответивших предметно на запрос, лишь два (Почта Банк и Связь-банк) сообщили, что раскрывают размер кредитной задолженности по овердрафтным картам по каждой операции. В

Абсолют Банке сообщили, что клиента информируют о наличии у него средств по-разному, в зависимости от категории карты. Так, если карта кредитная, то в балансе будут указаны только сумма доступных заемных средств. Если карта с разрешенным овердрафтом, то это будет сумма, включающая собственные средства держателя карты плюс доступные заемные средства.

В Совкомбанке пояснили, что уведомляют клиентов о проведении каждой операции, но не о размере кредитной задолженности перед кредитной организацией.

По словам председателя правления Международной конфедерации обществ потребителей (КонфОП) Дмитрия Янина, банки не заинтересованы в том, чтобы максимально оперативно доводить до заемщика информацию о его текущей задолженности (если он не в дефолте), так как каждая транзакция – это прибыль банка. По его мнению, обязательное уведомление заемщиков о сумме текущего долга будет сдерживать потребительские аппетиты и препятствовать появлению просроченной задолженности, которую заемщик не в состоянии погасить без нового займа. «Цель поправки – снизить вероятность перекредитования, и это очень важная поправка при условии, что банки не найдут способы обхода такого требования», – рассуждает он. Зампред правления Хоум Кредит Банка Александр Антоненко соглашается, что поправки сделают банковские кредитные продукты понятнее и «честнее для заемщика».

Последствия для банков

Вместе с тем банковские издержки на оповещение клиентов вырастут, сходятся во мнении опрошенные РБК банкиры. В Абсолют Банке и Совкомбанке отмечают, что им придется удлинить размер СМС-сообщений клиентам. «Из текста поправки непонятно, нужно ли уведомлять об общей сумме задолженности или о ближайшем платеже. Чтобы не путать, возможно, придется уведомлять и о том и другом. Конечно, после каждой покупки такие длинные сообщения на фоне постоянно растущей стоимости СМС-уведомлений – это очень дорого», – говорит первый зампред правления Совкомбанка Сергей Хотимский.

Нововведение может ощутимо увеличить расходы на фоне роста тарифов на такие услуги, говорят банкиры. Как писал РБК, с 1 февраля «МегаФон» поднял тарифы на СМС-рассылки, «ВымпелКом» (бренд «Билайн») – на одну из тарифных опций этой услуги. А МТС увеличила с декабря 2017 года стоимость СМС-рассылок для корпоративных клиентов.

Рост расходов банков на рассылки заставит их еще активнее переходить с СМС на пуш-уведомления, считает Сергей Хотимский.

Начальник аналитического управления Бинбанка Александр Свиридов соглашается, что изменение подхода к уведомлениям клиентов о задолженности приведет к росту операционных расходов кредиторов. Однако не для всех банков он будет значительным, добавляет он».

5.4.3. Комментарии к дополнениям в Уголовный кодекс

- **Парламентская газета – Кража денег с банковских карт может обернуться шестью годами тюрьмы**
  https://www.pnp.ru/social/krazha-deneg-s-bankovskikh-kart-mozhet-obernutsya-shestyu-godami-tyurmy.html

«Киберпреступников заставят чтить Уголовный кодекс

Законодатели намерены серьёзно усложнить жизнь жуликов, специализирующихся на краже денег с банковских карт. Госдума 27 марта приняла во втором чтении законопроект, который вводит в Уголовный кодекс специальный состав преступлений: за хищение с банковского счёта или воровство электронных денег предлагается установить наказание в виде лишения свободы на срок до шести лет.

Серьёзные хищения, весомые последствия

По информации Банка России, в 2016 году было совершено порядка 300 тысяч несанкционированных операций с использованием платёжных карт, эмитированных российскими банками, на общую сумму более миллиарда рублей. В прошлом году ущерб граждан от деятельности киберпреступников увеличился вдвое. При этом наблюдается постепенное сокращение доли несанкционированных операций с использованием банкоматов и платёжных терминалов и, напротив, устойчивый рост числа мошеннических операций в Интернете. Так, в 2016 году злоумышленники 717 раз покушались на счета юридических лиц на общую сумму 1,89 миллиарда рублей. В 50 процентах случаев деньги были списаны с клиентских счетов полностью или частично.

Российские парламентарии считают, что ужесточение наказания приведёт к реальному снижению уровня киберпреступности. Поясняя актуальность меры, глава Комитета Госдумы по финансовому рынку Анатолий Аксаков сказал, что многие воришки отделываются административными наказаниями, если списывают деньги со счетов небольшими суммами. При этом депутат обратил внимание, что в последние годы идёт резкое увеличение попыток нелегального списания средств.

«В прошлом году со счетов граждан украли два миллиарда рублей. Жёсткая уголовная ответственность позволит правоохранительным органам осуществлять оперативно-разыскную деятельность и обеспечить профилактику кражи средств с электронных счетов», – подчеркнул Анатолий Аксаков.

Согласно поправкам в Уголовный кодекс, кража с банковского счёта или кража электронных денежных средств будет наказываться штрафом в размере от 100 до 500 тысяч рублей, либо принудительными работами на срок до пяти лет с ограничением свободы до 1,5 года, либо к лишению свободы на срок до шести лет со штрафом в размере 80 тысяч рублей или с ограничением свободы на срок до 1,5 года.

Член Комитета Совета Федерации по экономической политике Антон Беляков убеждён, что выделение кражи с банковской карты в специальный состав преступлений, безусловно, норма полезная, но не бесспорная. При всей стройности законодательной логики сенатор видит возможные накладки, связанные с практической реализацией вводимой нормы.

В прошлом году со счетов граждан украли два миллиарда рублей. Жёсткая уголовная ответственность позволит правоохранительным органам осуществлять оперативно-разыскную деятельность и обеспечить профилактику кражи средств с электронных счетов.

«Сейчас очень популярной становится практика списания банком по запросу управляющей компании средств со счёта клиента. Для граждан это удобно – не нужно идти в банк и оплачивать коммунальные услуги. Всё происходит автоматически. Но представим

себе, что управляющая компания по ошибке списала завышенную сумму с жильцов многоквартирного дома. Внешне похоже на мошенничество, но по факту – только ошибка. Как в этом случае правоохранительные органы будут трактовать ситуацию? Вопрос, на который в процессе принятия законопроекта должны быть даны ответы. Невиновные пострадать не должны», – пояснил свою позицию парламентарий.

Закон не успевает за киберпреступниками

В то же время первый заместитель председателя Комитета Совета Федерации по экономической политике Сергей Калашников считает, что ужесточение наказания не окажет существенного влияния на уровень киберпреступности. Снизить его, считает парламентарий, можно лишь строго регламентировав пользование киберпространством.

«Во-первых, мировая и историческая практика показывает, что ужесточение наказания никак не влияет на уровень преступности. Во-вторых, киберпреступления – это настолько тонкая схема, в которую вовлечено огромное количество людей, что одним законодательным актом проблему не решить», – пояснил сенатор.

При этом уголовное законодательство обречено на отставание от совершенствующейся киберпреступности, считает Калашников. «Закон не успевает реагировать на постоянно меняющуюся технологическую ситуацию. Идёт, как говорится, вдогонку. А чтобы идти в ногу, необходимо устанавливать определённые правила игры для всех участников киберпространства. Нужно понять, что мы живём в новой реальности, которая требует новых форм регулирования. Нужно вводить новые определения, дефиниции и новые системы создания условий. Простой пример: введение нормы обязательного автострахования покончило с автоподставами», – пояснил он, допустив, что введение аналогичных норм в киберпространстве поможет снизить и количество преступлений в этой сфере.

Способы хищения с банковских карт

Эксперты связывают рост количества хищений денежных средств с банковских карт с несоблюдением гражданами элементарных правил безопасности. При этом преступники не топчутся на месте, а постоянно шлифуют свои навыки и разрабатывают новые схемы хищения.

Для кражи средств с банковских карт преступник чаще всего сегодня используют Интернет. Заражение вирусом-трояном операционной системы персонального компьютера или смартфона перенаправляет пользователя на поддельную веб-страницу, которая является точной копией банковского сайта. Здесь у ничего не подозревающего клиента выманивают персональные данные, которые впоследствии мошенники используют для входа в его личный кабинет на настоящем сайте банка и хищения средств.

Помимо этого существуют вирусные программы, которые встраиваются в браузер клиента и «на лету» меняют данные при произведении финансовых операций. Оплачивая коммунальные услуги, клиент не замечает, как вирус мгновенно подменяет номера счетов и даже суммы перечислений.

Киберпреступления – это настолько тонкая схема, в которую вовлечено огромное количество людей, что одним законодательным актом проблему не решить.

Другой способ обмана предполагает получение информации о банковской карточке клиента через фальшивые интернет-магазины аналоги известных и проверенных сайтов. Распространены также телефонные виды мошенничества, когда злоумышленники, взломав личный кабинет пользователя на сайте мобильного оператора, перенаправляют к себе на номер информацию от банка, получаемую клиентом.

Нередко мошенники используют совсем простые способы завладения информацией банковских клиентов. На номер, к которому привязана пластиковая карта, поступает смс-сообщение с информацией о блокировке карты и просьбой перезвонить по телефону для уточнения информации. Иногда доверчивые люди перезванивают по указанному номеру и предоставляют все данные, которые злоумышленники используют для опустошения счёта клиента.

2 миллиарда рублей в 2017 году украли злоумышленники со счетов россиян.

Установка накладных устройств для ввода ПИН-кода либо миниатюрных камер в банкоматах, способных считывать информацию с магнитных полос карты – ещё один способ получения персональной информации. Все эти ухищрения помогают злоумышленникам изготовить поддельные карты и использовать их для кражи средств.

Ранее «Парламентская газета» сообщала, что с 1 января 2018 года начал действовать утверждённый Центробанком национальный стандарт безопасности банковских и финансовых операций. В Банке России и Росстандарте считают, что переход на новые правила позволит финансовым организациям «повысить уровень защищённости от киберпреступлений, обеспечить стабильное и бесперебойное обслуживание клиентов». Кроме того, ЦБ ожидает, что новые стандарты безопасности существенно снизят риски в сфере кибербезопасности, связанные с несанкционированными транзакциями».

6. Кейс «Споры по платным сервисам»

Предоставление дополнительных услуг операторами связи регулируется Федеральным законом "О связи" (ссылка имеется в части 1 Сборника).

- **По адресу http://www.garant.ru/hotlaw/federal/485495/ размещен обзор Федерального закона N 229-ФЗ "О внесении изменений в Федеральный закон "О связи" от 23 июля 2013 г.**

«Операторы связи больше не смогут навязать дополнительные услуги абоненту.

Поправки направлены на борьбу с SMS-мошенничеством. Дело в том, что в 2012 г. возросло количество жалоб на услуги контент-провайдеров.

Большинство из них сводятся к следующему. Дополнительные услуги оказываются без согласия (акцепта) клиента, а также без предупреждения о размере платы за них. Кроме того, часто средства списывают за услуги, которые не были предоставлены.

Предусмотрено, что дополнительные услуги, технологически неразрывно связанные с услугами подвижной радиотелефонной связи, оказываются только с согласия абонента. Последнее должно быть выражено посредством совершения действий, однозначно идентифицирующих лицо (т. е. таких действий, которые позволяют достоверно установить волеизъявление клиента на получение услуг). Установлена ответственность операторов связи за несоблюдение этих требований.

До получения согласия абонента оператор связи должен предоставить ему информацию о тарифах и кратком содержании услуг.

Операторы могут привлекать к оказанию контентных услуг третьих лиц. По желанию абонента такие услуги оплачиваются с отдельного счета. Последний открывается на основании обращения лица.

Закреплено легальное определение контентных услуг.

Закон вступает в силу с 1 мая 2014 г.»

Текст закона от 23 июля 2013 г. N 229-ФЗ "О внесении изменений в Федеральный закон "О связи" доступен по ссылке http://base.garant.ru/70419130/, а полный текст закона "О связи" по ссылке http://base.garant.ru/70419130/.

6.1. Комментарии экспертов к положениям закона и судебная практика

6.1.1. Мнения, комментарии и консультации экспертов

- **LAWFIRM.ru – У мобильных операторов появятся новые обязанности при оказании контентных услуг http://www.lawfirm.ru/comments/index.php?id=5649**

«Совет Федерации одобрил Федеральный закон "О внесении изменений в Федеральный закон "О связи" (далее – Закон), которым урегулирован порядок оказания контентных услуг операторами подвижной радиотелефонной связи (далее – операторы). Под контентными услугами в Законе понимаются платные услуги, технологически неразрывно связанные с услугами подвижной радиотелефонной связи и направленные на повышение их потребительской ценности. В частности, к ним отнесены услуги по

предоставлению абонентам возможности получать в сетях связи справочную, развлекательную и (или) иную дополнительно оплачиваемую информацию, участвовать в голосовании, играх, конкурсах и аналогичных мероприятиях. На стадии рассмотрения Госдумой данный Закон проходил как проект Федерального закона N 263437-6. В случае подписания Президентом РФ Закон вступит в силу с 1 мая 2014 г.

Операторов обяжут предварительно проинформировать абонента об условиях оказания контент-услуг

В соответствии с Законом перед тем, как абонент даст согласие на оказание ему услуг, оператор связи обязан проинформировать его о тарифах на услуги, их кратком содержании, предоставляющем их лице и лицевом счете, с которого будут списываться денежные средства на оплату услуг. Отметим, что способ такого информирования в Законе не установлен. Вероятно, информация может высылаться непосредственно абоненту (например, посредством СМС-сообщений или на электронную почту) либо размещаться в СМИ или на официальном сайте оператора. Услуги, об условиях оказания которых абонент не был проинформирован, не должны будут оплачиваться.

Напомним, что в настоящее время требования об информировании потребителя об услуге содержатся в ст. 10 Закона РФ от 07.02.1992 N 2300-1 "О защите прав потребителей" (далее – Закон N 2300-1). За нарушение права потребителя на получение информации об оказываемой ему услуге в ст. 14.8 КоАП РФ предусмотрена административная ответственность в виде штрафа, размер которого для юрлиц составляет от 5000 до 10 000 руб. Для абонентов, не являющихся потребителями, подобных норм не установлено.

Согласно Закону за непредоставление информации операторы будут нести гражданско-правовую ответственность перед абонентами.

Операторы будут открывать отдельные лицевые счета по желанию абонента для оплаты контент-услуг

Нововведением Закона стало установление обязанности оператора, оказывающего контентные услуги с привлечением третьих лиц (например, контент-провайдеров), создавать по обращению абонента отдельный лицевой счет для оплаты названных услуг. При этом размер средств, направляемых на оплату услуг, будет ограничен суммами, находящимися на указанном лицевом счете. Можно предположить, что у мобильных операторов возникнут дополнительные расходы по обслуживанию отдельного абонентского счета. Поэтому вполне вероятно, что такие расходы могут вызвать повышение стоимости предоставляемых абоненту контент-услуг.

Выражение согласия абонента на получение контент-услуг должно позволять точно определить его личность и волеизъявление

В соответствии с п. п. 8 и 21 Правил оказания услуг подвижной связи (утв. Постановлением Правительства РФ от 25.05.2005 N 328) предоставление услуг подвижной связи может с согласия абонента сопровождаться оказанием иных услуг, технологически неразрывно связанных с услугами подвижной связи и направленных на повышение их потребительской ценности. Кроме того, в п. 3 ст. 16 Закона N 2300-1 установлен запрет оказания дополнительных услуг без согласия потребителя. Данные нормы применяются на практике и при оказании услуг подвижной радиотелефонной связи (см., например, Определение Свердловского областного суда от 13.08.2012 по делу N 33-9753/2012).

Тем не менее до сегодняшнего дня способ выражения согласия абонента на оказание услуг не урегулирован. В соответствии с Законом абонент должен выразить свое согласие только путем совершения действий. При этом должна быть обеспечена возможность достоверно установить его личность и волеизъявление на получение услуги. В настоящее время суды признают согласием абонента на оказание контентных услуг такие действия, как, например, направление СМС-сообщения на номер, содержащийся в оферте (см. Определение Московского городского суда от 26.12.2011 по делу N 4г/5-1077511), верификация телефонного номера на сайте и пополнение виртуального счета под своим аккаунтом (см. Постановление ФАС Западно-Сибирского округа от 25.05.2012 по делу N А03-10143/2011), указание своего номера телефона при регистрации на сайте в целях активации подписки на платные сервисы и последующий ввод кода, полученного абонентом в СМС-сообщении (Апелляционное определение Московского городского суда от 30.08.2012 по делу N 11-18639). Кроме того, вероятно, согласие может быть выражено путем подписания с оператором соглашения на бумажном носителе или в электронной форме.

Услуги, оказанные с нарушением перечисленных требований, не будут подлежать оплате. Наряду с этим согласно Закону за нарушение этих требований операторы будут нести гражданско-правовую ответственность перед абонентами (например, в виде возмещения убытков и компенсации морального вреда).

Федеральный закон "О внесении изменений в Федеральный закон "О связи"

С текстом проекта Федерального закона N 263437-6 к третьему чтению можно ознакомиться на сайте Госдумы (http://asozd2.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=263437-6)».

- **Роспотребнадзор – Комментарии**
  http://77.rospotrebnadzor.ru/index.php/napravlenie/zpp/2863-2015-03-13-07-17-23

«Наиболее распространенными проблемами, выявляемыми в области подвижной связи при рассмотрении обращений граждан, являются действия операторов, навязывающих и подключающих контентные услуги без согласия абонента. Изменения норм Федерального Закона «О связи», касающиеся порядка предоставления контентных услуг, вступили в силу только с 1 мая 2014 года.

В соответствии с изменениями в Федеральный Закон «О связи» введено понятие «контентные услуги».

Контентные услуги - вид услуг связи, которые технологически неразрывно связаны с услугами подвижной радиотелефонной связи и направлены на повышение их потребительской ценности (в том числе услуги по предоставлению абонентам возможности получать на пользовательское (оконечное) оборудование в сетях связи справочную, развлекательную и (или) иную дополнительно оплачиваемую информацию, участвовать в голосовании, играх, конкурсах и аналогичных мероприятиях) и стоимость оказания которых оплачивается абонентом оператору связи, с которым у абонента заключен договор об оказании услуг связи. Это чаще всего услуги, оказываемые с «коротких номеров».

Законом устанавливается возможность их подключения только при совершении абонентом действий, однозначно идентифицирующих абонента и позволяющих достоверно

установить его волеизъявление, что, как ожидается, поможет более эффективно отстаивать права потребителя. Основная проблема надзора в данной области состоит в том, что мнение оператора связи о возникшей спорной ситуации и формальные показания средств измерений оператора (то есть обстоятельства, не имеющие достаточной объективности) зачастую возводятся в ранг неоспоримых доказательств. Если же Вы обнаружили снятие с Вашего счета «лишних денег», то в соответствии с Правилами оказания услуг телефонной связи (утв. постановлением Правительства Российской Федерации от 9 декабря 2014 г. N 1342) Абонент вправе:

– отказаться от оплаты услуг телефонной связи, предоставленных ему без его согласия;
– требовать перерасчет денежных средств, вплоть до полного возврата сумм, уплаченных за услуги телефонной связи, вследствие непредставления услуг телефонной связи не по вине абонента или предоставления их ненадлежащего качества;
– получать дополнительную информацию об оказанных услугах телефонной связи (детализацию счета), в том числе с указанием даты и времени установления соединений, их продолжительности и абонентских номеров (п. 26 Правил).

На основании данных норм Вы вправе затребовать у Оператора детализацию счета с указанием наименования услуги, объема и ее стоимости. Если Вы не заказывали такую услугу, в т.ч. не совершали конклюдентных действий, или фактически не получали, потребовать произвести перерасчет стоимости услуг, а при неисполнении Вашего требования – обратиться в суд.

В соответствии со ст. 11 Гражданского Кодекса Российской Федерации и ст.17 Закона Российской Федерации «О защите прав потребителей» защита нарушенных гражданских прав, рассмотрение имущественных споров находится в компетенции суда. Иски о защите прав потребителей могут быть предъявлены по выбору истца в суд по месту: нахождения организации; жительства или пребывания истца; заключения или исполнения договора. Потребители по искам, связанным с нарушением их прав, освобождаются от уплаты государственной пошлины. В суде Вы можете использовать свидетельские показания. По Вашему заявлению».

- **РБК – Счет от греха подальше**
  https://www.rbc.ru/newspaper/2013/01/18/56c1c8109a7947ac7f7ac254

«Роскомнадзор предложил платить за контент-сервисы отдельно от услуг связи

Как стало известно РБК daily, Роскомнадзор требует от операторов принять дополнительные меры по борьбе с недобросовестными контент-провайдерами. Вчера на встрече регулятор предложил им сделать отдельный абонентский счет для оплаты контент-услуг. Участники рынка выражают опасение, что эта мера не решит проблемы мошенничества, а лишь ограничит доступ к социально значимым сервисам.

Регулятор предложил операторам подумать о двух мерах по борьбе с мошенничеством с короткими номерами. Во-первых, речь идет о создании второго абонентского счета для оплаты контент-услуг, чтобы те, кому они не нужны, не могли случайно потратить средства в пользу мошенников. Во-вторых, предлагается прекратить продажу SIM-карт в помещениях площадью меньше 20 кв. м в городах и меньше 10 кв. м – в сельской местности. Об этом РБК daily рассказал представитель Роскомнадзора Владимир Пиков. На следующей встрече операторы смогут дать оценку этим идеям, добавил он.

Также на совещании операторы отвергли идею регулятора по заключению бумажных договоров на оказание контент-услуг.

Операторы неоднозначно оценивают идеи Роскомнадзора. «По сути предложения регулятора мало чем помогут: ранее провайдеры, например, рассылали вирусы и вредоносное ПО, отправляющие платные SMS с основного баланса, теперь они это будут делать по-другому – с дополнительного баланса», – считает один из участников совещания. Сами операторы выдвигали конструктивные предложения по изменению законодательства, но они почему-то не были восприняты Роскомнадзором, уверяет он.

«Данное предложение (по разделению абонентских счетов. – РБК daily) Роскомнадзора серьезно усложнит для абонентов процесс пользования допуслугами и, помимо этого, потребует затрат на перестройку систем от операторов», – заявила представитель «ВымпелКома» Анна Айбашева.

Разделение счетов затруднит оплату в социально важных сервисах, указывает представитель МТС Валерия Кузьменко. «Например, контент-сервисы позволяют гражданам отправлять жалобы президенту по SMS, оплачивать парковки, получать доступ к расписанию транспорта, участвовать в благотворительных проектах, интерактивной поддержке масштабных телевизионных проектов», – поясняет она.

МТС и «ВымпелКом» сходятся во мнении, что предупреждения ФАС, полученные в декабре прошлого года, уже способствуют предотвращению мошенничества. ФАС провела проверку операторов по жалобам на мошенничество через контент-сервисы, обязав операторов информировать абонентов о стоимости сервисов и возможной подписке на них. Эти меры полностью обеспечивают прозрачность предоставления контентных сервисов без изменения законодательства, считают оба оператора.

«Инициативы направлены на защиту абонентов и операторов, в этом мы согласны с регулятором. Детали реализации предложенных мер требуют тщательного анализа», – сказал начальник департамента «МегаФона» по борьбе с мошенничеством Сергей Хренов, участвовавший в совещании».

- **CNEWS – Сотовые операторы нашли лазейку в законе «О мобильном мошенничестве»**
  http://www.cnews.ru/news/top/sotovye_operatory_nashli_lazejku_v_zakone

«Корреспондент CNews Игорь Королев в ходе тестирования предусмотренной поправками к закону «О связи» возможности защититься от мобильных мошенников открыл второй счет для контент-услуг. Однако оказалось, что все три сотовых оператора по-прежнему снимают деньги за брендированные контент-сервисы с основного счета.

С 1 мая 2014 г. вступили в силу поправки к закону «О связи», в соответствие с которыми при оказании контент-услуг сотовые операторы обязаны предварительно информировать абонента об их стоимости и получать согласие на оказание услуг в явном виде (Advice of charge, AOC). Кроме того, абонент вправе завести отдельный (второй) счет для оплаты контент-услуг.

Корреспондент CNews решил протестировать эту возможность у трех крупнейших сотовых операторов: «Билайн», МТС и «Мегафон». Оказалось, что узнать у сотрудников самих операторов информацию об открытии второго счета не так-то просто, а у МТС, в

отличие от двух других операторов, второй счет нельзя открыть дистанционно: требуется личное посещение офиса и подача письменного заявления.

Тем не менее, собрав всю необходимую информацию, корреспондент принялся непосредственно открывать вторые счета. Первый делом он попытался завести дополнительный счет у «Мегафона». Для этого, по словам сотрудников оператора, достаточно было ввести USSD-команду. Но система ответила отказом. Повторив попытку через некоторое время, корреспондент в ответ получил SMS со следующим текстом: «Вы подписались на викторину «Тепло/холодно». 3 руб/день».

Оказалось, что при открытии счета был введен неверный USSD-номер. Правда, по идее, в соответствие с новым законом «Мегафон» сначала должен был предупредить абонента, что он подключает платную услугу, однако ее включили автоматом.

Второй счет корреспондент CNews все же завел, но деньги на него не положил, ожидая, что средства за викторину с его основного счета списываться также не будут. Однако баланс основного счета уменьшался на 3 рубля в день. То есть, пытаясь защититься от контент-услуг, абонент, наоборот, «попал» на одну из них.

Корреспондент решил обсудить эту проблему с абонентской службой «Мегафона». Девушка-оператор взяла паузу, потом вернулась и уточнила, уверен ли он в отсутствии денег на втором счете и какой командой он проверял его баланс. Затем оператор колл-центра вновь отлучилась и, наконец, вынесла свой вердикт:

– При отсутствии денег на втором счете они списываются с основного. Спасибо за понимание!

В чем тогда смысл второго счета, если деньги все равно могут списываться с первого, сотрудница оператора не пояснила. «Тайну» раскрыл директор по новым услугам «Мегафона» Дмитрий Юмашев:

– Изменения в законе «О связи» относятся только к услугам сторонних контент-провайдеров. Услуги же, предоставляемые непосредственно оператором, по-прежнему можно оказывать без АОС, а деньги за них списывать с основного счета.

Забегая вперед, надо отметить, что такая же ситуация и в МТС, и в «Билайне». Между тем, так называемые «брендированные» услуги (под брендами операторов) зачастую оказываются все теми же сторонними контент-провайдерами, только избранными. У «Билайна» это его главный партнер в мобильном контенте - «Темафон», а МТС право предоставления услуг под его брендом разыгрывает на тендере.

Если не учитывать этот нюанс, второй счет в «Мегафоне» работает нормально. Деньги на него переводятся с основного счета USSD-командой, баланс также проверяется на телефоне другой командой. Сторонние подписки активируются, но средства при нулевом балансе второго счета за них не списываются.

Далее корреспондент CNews приступил к тестированию второго счета в МТС. Для этого, напомним, требовалось направлять письменное заявление и ждать до 10 дней. В нашем случае счет был заведен на следующий день. Об этом корреспонденту CNews сообщили в абонентской службе. Проверив его паспортные данные, девушка-оператор продиктовала длинный номер. Это номер лицевого счета, через который и следует пополнять счет для контент-услуг, пояснила она.

Вот только как пополнить номер по 11-значному номеру лицевого счета, девушка не пояснила. Скажем, в терминалах Qiwi есть только поле для ввода 10-значного номера телефона. Далее обнаружилось, что не понятно, как вообще проверить баланс второго счета: на сайте в личном кабинете он не отображался.

На странице МТС раздел про второй счет отсутствует: вместо этого предлагается прочитать огромный договор об оказании контент-услуг. В договоре ответ нашелся: если не подключена услуга «Управление номерами», то и баланс второго счета не будет отображаться в личном кабинете.

Эту услугу можно подключить бесплатно. После этого в личном кабинете появляется второй номер. Оказывается, что он сильно похож на первый, только вместо первой цифры кода - «9» - там цифра «1». Такого рода измененные номера используются для пополнения отдельного счета мобильной коммерции.

После перевода 100 руб на номер с кодом «116» на контент-счете действительно появились деньги. Вот только для тестирования мне нужно было, чтобы средств там не было. О возможности перевода средств между основным и вторым счетом нигде ничего не сообщалось, поэтому для «обнуления» счета пришлось покупать дорогую mp3-мелодию. Впоследствии выяснилось, что перевод средств между счетами все-таки возможен – для этого существует специальная USSD-команда, вот только знают о ней почему-то только в пресс-службе МТС.

Следующим тестированию подвергся «Билайн». Здесь, как и в «Мегафоне», второй счет открывается USSD-командой. В ответ на команду система выдала отказ с предложением обратиться в техподдержку. Молодой человек в колл-центре взял паузу и вернулся с неожиданным ответом:

– У вас уже есть заявка на открытие второго счета, второй раз ее отправить нельзя.

Очевидно, он ошибся. Впрочем, история «боев» с МТС за открытие второго счета «закалила» корреспондента CNews и он стал пробовать другие способы активации. Выяснилось, что в личном кабинете второй счет возможно открыть буквально за минуту. Помимо этого есть способ открытия счета по звонку на специальный IVR-номер.

Пополнить второй счет в «Билайне» можно переводом на тот же телефонный номер, только вместо первой цифры «9» необходимо указывать цифру «6». Возможен и перевод между счетами. Баланс второго счета просматривается как в личном кабинете, так и на телефоне (с помощью специальной USSD-команды). Разовые контент-запросы при нулевом балансе второго счета совершить не удается, сторонние подписки цепляются, но через день, за неимением средств, их отключают.

Возможности второго счета для контент-услуг

	МТС	«Мегафон»	«Билайн»
Возможность дистанционной активации второго счета:	-	+	+
– USSD-команда		+	+

– личный кабинет		+	+
– IVR		-	+
Просмотр баланса второго счета в личном кабинете	+/- (*)	+	+
Просмотр баланса на телефоне	+	+	+
Прямой перевод денег на второй счет	+	-	+
Перевод денег между счетами	+	+	+

(*) при подключении дополнительной услуги «Управление номерами»

Подводя итог: сотовые операторы долго сопротивлялись регулированию рынка контент-услуг, угрожая, что борьба с мобильным мошенничеством негативно отразиться на легальных сервисах и на доходах самих операторов. Тем не менее, закон приняли, и его пришлось исполнять. Но операторы пошли на «хитрость» и вывели из-под его действия брендированные услуги.

Конечно, это все равно шаг вперед. Мошеннических услуг под брендами операторов оказываться не будет, и абоненты, заведя второй счет с нулевым балансом, могут быть уверены, что деньги «за воздух» они не отдадут. Вот только риск случайно попасть на легальную платную услугу, которая на самом деле не нужна была пользователю, все равно остается.

Остается и фактор неосведомленности пользователей о самой возможности открытия второго счета. Правда, по крайней мере в «Билайне», пообещали проинформировать своих пользователей о такой возможности путем проведения SMS-рассылки.

Объемная консультация по вопросам судебной практики по договору возмездного оказания услуг содержится по адресу: https://rusjurist.ru/sudebnaya_praktika/sudebnaya_praktika_po_dogovoru_vozmezdnogo_okazaniya_uslug/».

6.1.2. Решения судов

Обратите внимание, что судебная практика по этим вопросам неоднозначна.

- **Решение № 2-91/2018 2-91/2018 ~ М-69/2018 М-69/2018 от 17 мая 2018 г. по делу № 2-91/2018**

Ивнянский районный суд (Белгородская область) – Гражданские и административные

Дело № 2-91/2018

Р Е Ш Е Н И Е

И М Е Н Е М Р О С С И Й С К О Й Ф Е Д Е Р А Ц И И

п. Ивня 17 мая 2018 года

Ивнянский районный суд Белгородской области в составе:

председательствующего судьи Бойченко С.И. при секретаре Брусенской О.И.,

в открытом судебном заседании рассмотрел дело по исковому заявлению Погожевой Татьяны Анатольевны к ПАО «Вымпел-Коммуникации» о признании незаконными действий по подключению дополнительных платежных услуг телефонной связи, взыскании денежных средств, компенсации морального вреда, штраф

УСТАНОВИЛ:

Истец обратилась в суд с иском к ПАО "Вымпел-Коммуникации" о признании действий незаконными, компенсации морального вреда, штрафа в связи со следующими обстоятельствами.

Погожева указала о том, что она является абонентом сотовой связи "Биллайн". Расходы на оплату мобильной связи истца составляли не более 250 рублей в месяц, однако с начала 2017 года они возросли, несмотря на то, что время разговоров и количество СМС сообщений осталось прежним. При изучении детализации расходов истца было установлено, что с нее взималась плата за дополнительные услуги – информационно-развлекательные сервисы «Обнаженная натура», «Биллайн. Книги». По утверждению истца она данные услуги не подключала, ее телефон не имеет технической возможности пользоваться указанными услугами так как доступа к Интернету он не имеет. По данному факту истец обратилась к ответчику и получила ответ подтверждающий факт подключения ей вышеуказанных услуг с 16.11.2016 г. по 14.05.2017 г., однако в добровольном порядке истцу было отказано в возврате взимаемой платы за дополнительные услуги. В связи с изложенным истец просила суд признать незаконными действий по подключению дополнительных платежных услуготелефонной связи, взыскать денежные средства в размере 1742,53 р., компенсацию морального вреда в размере 5000 руб., штрафа в размере 50 % от присужденной судом суммы и взыскать понесенные ею судебные расходы по оплате услуг адвоката в размере 4000 рублей и почтовые расходы в сумме 43 рубля.

Истец в судебное заседание не явился о времени месте рассмотрения дела уведомлен надлежащим образом, в представленном в суд заявлении требования поддержала, просила их удовлетворить в полном объеме.

Возражений относительно заявленных требований не представил.

Ответчики в судебное заседание не явились, извещены о времени и месте рассмотрения дела надлежащим образом, возражений по иску не представили. С учетом отсутствия со стороны истца возражений против рассмотрения дела в порядке заочного производства, дело рассматривается в порядке заочного производства.

Заслушав истца, исследовав материалы дела, суд приходит к следующим выводам.

Истец Погожева обратилась в суд с требованиями к ПАО "Вымпел-Коммуникации", просила суд признать незаконными действий по подключению дополнительных платежных услуг телефонной связи, взыскать денежные средства в размере 1742,53 р.,

компенсацию морального вреда в размере 5000 руб., штрафа в размере 50 % от присужденной судом суммы и взыскать понесенные ею судебные расходы по оплате **услуг** адвоката в размере 4000 рублей и почтовые расходы в сумме 43 рубля.

В материалах дела содержится ответ на претензию истца ПАО "ВымпелКом" от 03.09.2017 года, в котором ответчик сообщает Погожевой о том, что факт подключения ей спорных **услуг** имел место быть с 16.11.2016 г. по 14.05.2017 г., в добровольном порядке истцу было отказано в возврате взимаемой платы за дополнительные **услуги** (л.д. 9-10).

В соответствии с пунктом 3 статьи 16 Закона "О защите прав потребителей" продавец (исполнитель) не вправе без согласия потребителя выполнять дополнительные работы, **услуги** за плату. Потребитель вправе отказаться от оплаты таких работ (услуг), а если они оплачены, потребитель вправе потребовать от продавца (исполнителя) возврата уплаченной суммы. Согласие потребителя на выполнение дополнительных работ, **услуг** за плату оформляется продавцом (исполнителем) в письменной форме, если иное не предусмотрено федеральным законом.

Постановлением Правительства Российской Федерации от 09.12.2014 N 1342 утверждены Правила оказания **услуг** телефонной связи (далее – Правила оказания **услуг** телефонной связи), которые регулируют отношения между абонентом и (или) пользователем услуг телефонной связи и оператором связи при оказании **услуг** местной, внутризоновой, междугородной и международной телефонной связи в сети связи общего пользования, а также при оказании **услуг** подвижной радиосвязи, **услуг** подвижной радиотелефонной связи и услуг подвижной спутниковой радиосвязи в сети связи общего пользования.

При этом под абонентом понимается пользователь **услуг** телефонной связи, с которым заключен договор об оказании **услуг** телефонной связи при выделении для этих целей абонентского номера или уникального кода идентификации.

Под абонентским номером понимается телефонный номер, однозначно определяющий (идентифицирующий) оконечный элемент сети связи или подключенную к сети подвижной связи абонентскую станцию (абонентское устройство) с установленным в ней (в нем) идентификационным модулем.

В силу п. 1 ст. 44-ФЗ "О связи" **услуги** связи оказываются операторами связи пользователям **услугами** связи на основании договора об оказании **услуг** связи, заключаемого в соответствии с гражданским законодательством и правилами оказания **услуг** связи. Сторонами по договору выступают гражданин, юридическое лицо или индивидуальный предприниматель, с одной стороны, и оператор связи, с другой стороны (пункт 14 Правил оказания **услуг** телефонной связи).

В соответствии с пунктом 24 Правил оказания **услуг** телефонной связи оператор связи обязан: а) оказывать абоненту и (или) пользователю **услуги** телефонной связи в соответствии с законодательными и иными нормативными правовыми актами Российской Федерации, настоящими Правилами, лицензией и договором; б) устранять в сроки, установленные оператором связи, неисправности, препятствующие пользованию **услугами** телефонной связи. Информация о сроках устранения неисправностей, препятствующих пользованию **услугами** связи, размещается на сайте оператора связи в информационно-телекоммуникационной сети "Интернет"; в)

возобновлять оказание услуг телефонной связи абоненту в течение 3 дней со дня получения оплаты от абонента или предоставления абонентом документов, подтверждающих ликвидацию задолженности по оплате услуг телефонной связи (в случае приостановления оказания услуг телефонной связи за нарушение сроков оплаты оказанных ему услуг телефонной связи); г) по требованию абонента или пользователя предоставлять дополнительную информацию, связанную с оказанием услуг телефонной связи; д) вернуть абоненту неиспользованный остаток денежных средств, внесенных в качестве аванса, не позднее 30 дней со дня расторжения договора; е) не менее чем за 10 дней до изменения действующих тарифов на услуги телефонной связи извещать об этом абонентов через сайт оператора связи.

В силу ч. 1 ст. 56 ГПК РФ, каждая сторона должна доказать те обстоятельства, на которые она ссылается как на основания своих требований и возражений, если иное не предусмотрено федеральным законом.

Судом у ответчика истребовались сведения о детализации счета истца за период с 01.11.2016 г. по 14.05.2017 г. включительно, однако, ответчик суду их не представил, уклонился от представления доказательств по делу.

Таким образом, суду не представлено доказательство, на котором основаны оспариваемые истцом действия ПАО "ВымпелКом" по списанию денежных средств, поэтому суд не может сделать вывод о законности таких действий.

В такой ситуации суд находит обоснованными исковые требования истца к ответчику ПАО "ВымпелКом", поскольку именно эта организация оказывает истцу услуги связи и осуществила списание его денежных средств.

В соответствии с ч. 1 ст. 48 ГК РФ, юридическим лицом признается организация, которая имеет обособленное имущество и отвечает им по своим обязательствам, может от своего имени приобретать и осуществлять гражданские права и нести гражданские обязанности, быть истцом и ответчиком в суде. В рассматриваемой ситуации именно юридическое лицо - ПАО "ВымпелКом", осуществив оспариваемые истцом действия в отсутствие подтвержденных оснований для списания денежных средств со счета Погожевой, нарушило права истца.

Пунктом 8 статьи 68 ФЗ "О связи" прямо предусмотрено, что операторы связи несут ответственность перед абонентами за нарушение требований, установленных пунктом 5 статьи 44 настоящего закона, при подключении и предоставлении иных услуг связи, технологически неразрывно связанных с услугами подвижной связи и направленных на повышение их потребительской ценности, в том числе контентных услуг.

В соответствии с п. 5 ст. 54 ФЗ "О связи" о связи не подлежат оплате иные услуги связи, технологически неразрывно связанные с услугами подвижной радиотелефонной связи и направленные на повышение их потребительской ценности, в том числе контентные услуги, оказанные с нарушением требований, установленных настоящим Федеральным законом.

В силу ст. 15 Закона "О защите прав потребителей" моральный вред, причиненный потребителю вследствие нарушения изготовителем (исполнителем, продавцом, уполномоченной организацией или уполномоченным индивидуальным предпринимателем, импортером) прав потребителя, предусмотренных законами и правовыми актами

Российской Федерации, регулирующими отношения в области защиты прав потребителей, подлежит компенсации причинителем вреда при наличии его вины. Размер компенсации морального вреда определяется судом и не зависит от размера возмещения имущественного вреда. Компенсация морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных потребителем убытков.

Действиями оператора связи нарушены права потребителя, соответственно, требование истца о компенсации морального вреда является законным и обоснованным.

В соответствии со ст. 1101 Гражданского кодекса РФ, размер компенсации морального вреда определяется судом в зависимости от характера причиненных потерпевшему физических и нравственных страданий, а также степени вины причинителя вреда в случаях, когда вина является основанием возмещения вреда. При определении размера компенсации вреда должны учитываться требования разумности и справедливости. В каждом конкретном случае при решении вопроса о компенсации морального вреда судом должны учитываться все заслуживающие внимания обстоятельства. В данном случае суд находит, что требованиям разумности и справедливости при определении размера компенсации морального вреда соответствует сумма в размере 5 000 рублей.

В п. 46 постановления Пленума Верховного Суда Российской Федерации от 28 июня 2012 года N 17 "О рассмотрении судами гражданских дел по спорам о защите прав потребителей" разъяснено, что при удовлетворении судом требований потребителя в связи с нарушением его прав, установленных Законом о защите прав потребителей, которые не были удовлетворены в добровольном порядке, суд взыскивает с ответчика в пользу потребителя штраф независимо от того, заявлялось ли такое требование суду (п. 6 ст. 13 Закона).

Учитывая, что требования истца не были удовлетворены в добровольном порядке, с ПАО "ВымпелКом" в пользу истца подлежит взысканию штраф в размере пятьдесят процентов от суммы, присужденной судом в пользу потребителя.

Претензией к ответчику, ордером адвоката и квитанциями об оплате **услуг** адвоката и почтовой связи (л.д. 8-9, 22) подтверждается, что истец понесла судебные расходы по оплате **услуг** адвоката в размере 4000 рублей и почтовые расходы в сумме 43 рубля, которые в соответствии со ст. 98 ГПК РФ подлежат взысканию с ответчика в пользу истца.

В соответствии со ст. 103 ГПК РФ, с ответчика следуетвзыскатьгоспошлину в доход бюджета муниципального образования «Ивнянский район» в размере 700 руб. 00 коп., исходя из существа удовлетворенных исковых требований.

Учитывая изложенное, руководствуясь ст. ст. 194 - 199 ГПК РФ, суд

РЕШИЛ:

Исковые требования Погожевой Татьяны Анатольевны к ПАО «Вымпел-Коммуникации» о признании незаконными действий по подключению дополнительных платежных **услуг** телефонной связи, взыскании денежных средств, компенсации морального вреда, штрафа – удовлетворить.

Взыскать с ПАО "Вымпел-Коммуникации" в пользу Погожевой Татьяны Анатольевны уплаченную денежную сумму в размере 1742,53 руб.,компенсацию морального вреда в размере 5 000 рублей, штраф в размере 3371,26 руб.

Взыскать с ПАО "Вымпел-Коммуникации" в пользу Погожевой Татьяны Анатольевны судебные расходы по оплате **услуг** адвоката в размере 4000 рублей и почтовые расходы в сумме 43 рубля.

Взыскать с ПАО "Вымпел-Коммуникации" госпошлину в доход бюджета муниципального образования «Ивнянский район» в сумме 700 рублей.

Ответчик вправе подать в суд, принявший заочное решение, заявление об отмене этого решения суда в течение семи дней со дня вручения ему копии этого решения. Заочное решение суда может быть обжаловано сторонами также в апелляционном порядке в течение месяца по истечении срока подачи ответчиком заявления об отмене этого решения суда, а в случае, если такое заявление подано, - в течение месяца со дня вынесения определения суда об отказе в удовлетворении этого заявления.

Судья – подпись - С.И. Бойченко

- **Определение**
  Дело № 11-154/2018

Мировой судья Пахоменкова М.А.

АПЕЛЛЯЦИОННОЕ ОПРЕДЕЛЕНИЕ

11 июля 2018 года г. Смоленск

Ленинский районный суд г. Смоленска

в составе:

председательствующего судьи Манакова В.В.,

при секретаре Якубенковой С.А.,

рассмотрев в открытом судебном заседании апелляционную жалобу Лосева Игоря Владимировича на решение мирового судьи судебного участка №8 в г. Смоленске от 24.04.2018,

установил:

Лосев И.В. обратился в суд с иском к ПАО «МТС», ООО «Стрим» о взыскании денежных средств, компенсации морального вреда, возмещении судебных расходов. В обоснование указав, что является абонентом ПАО «МТС» с номером №, которым пользуется только для получения услуг интернета. В июне 2017 года истец произвел сверку расчетов по данному номеру, в результате выявилась переплата в размере 14 998 руб. 90 коп., которая списывалась за счет непредусмотренных тарифом услуг. Кроме того, в январе 2016 года и сентябре 2016 года при переходе на другой тариф с него сняли двойную оплату в размере 350 руб. ДД.ММ.ГГГГистец обратился с письменной претензией в ПАО «МТС», по результатам рассмотрения которой ДД.ММ.ГГГГ частично удовлетворены его требования на сумму 1700 руб. Уточнив требования, просит взыскать с ПАО «МТС» денежные средства за двойную оплату тарифов в январе 2016 года в размере 350 руб., денежные средства за двойную оплату тарифов в сентябре 2016 года в размере 350 руб., денежные средства взысканные за услугу «Интернет на день» в размере 150 руб., денежные средства за не оказанную услугу «Гудок» в размере 196 руб., денежные средства за не оказанную услугу «Вам звонили» в размере 18 руб. 90 коп., денежные средства за не

оказанную услугу «Подписка МТС ТВ» в размере 6 360 руб., денежные средства за не оказанную услугу «Режим модема» в размере 3 910 руб., денежные средства в размере 50% от суммы не оказанных услуг в размере 5 667 руб. 45 коп.; взыскать в солидарном порядке с ПАО «МТС» и ООО «Стрим» в свою пользу денежные средства за не оказанную услугу «Подписка 1158» в размере 340 руб., денежные средства за не оказанную услугу «Подписка 0001» в размере 1 260 руб., денежные средства за не оказанную услугу «Подписка 9224» в размере 1 080 руб., денежные средства в размере 50% от суммы не оказанных услуг в размере 1 340 руб., компенсацию морального вреда в размере 9 000 руб., в счет возмещения судебных расходов 9 000 руб.; признать недействительными п.2 Правил подписки на контент сайта adultvidos.ru в части: В случае неполучения от Абонента отказа от Подписки на Контент, срок предоставления Подписки на Контент автоматически продлевается каждый раз на 1 день до момента самостоятельного отключения Абонентом Подписки на Контент; п. 2 Правил подписки на контент сайта ozornica.com в части: В случае неполучения от Абонента отказа от Подписки на Контент, срок предоставления Подписки на Контент автоматически продлевается каждый раз на 2 дня до момента самостоятельного отключения Абонентом Подписки на Контент; п.2 Правил подписки на контент сайта playfullvideo.ru в части: В случае неполучения от Абонента отказа от Подписки на Контент, срок предоставления Подписки на Контент автоматически продлевается каждый раз на 1 день до момента самостоятельного отключения Абонентом Подписки на Контент; п.8.5 Порядка предоставления контентных услуг МТС в части: В случае нежелания Абонента пользоваться Периодической Контентной услугой с ограничениями, указанными в настоящем Порядке, Абонент вправе отключить такую услугу в порядке, указанном в п.4.2 настоящего Порядка. До момента отключения Периодической Контентной услуги Абонент обязан оплачивать такую услугу в размере и порядке согласно разделу 5 настоящего Порядка.

Определением мирового судьи судебного участка №8 в г.Смоленске от ДД.ММ.ГГГГ принят отказ Лосева И.В. от части исковых требований, а именно: взыскать с ПАО «МТС» в пользу Лосева И.В. денежные средства, взысканные за услугу ИНТЕРНЕТ НА ДЕНЬ в размере 150 руб.; взыскать с ПАО «МТС» в пользу Лосева И.В. денежные средства за не оказанную услугу ГУДОК в размере 196 руб.; взыскать с ПАО «МТС» в пользу Лосева И.В. денежные средства за не оказанную услугу ВАМ ЗВОНИЛИ в размере 18,9 руб.; взыскать солидарно с ПАО «МТС», ООО «Стрим» в пользу Лосева И.В. за не оказанную услугу Подписку 1158 денежные средства в размере 340 руб.; взыскать солидарно с ПАО «МТС», ООО «Стрим» в пользу Лосева И.В. за не оказанную услугу Подписку 0001 денежные средства в размере 1260 руб.; взыскать солидарно с ПАО «МТС», ООО «Стрим» в пользу Лосева И.В. за не оказанную услуг Подписку 9224 денежные средства в размере 1080 руб. Производство по делу в данной части иска прекращено.

Решением мирового судьи судебного участка №8 в г.Смоленске от ДД.ММ.ГГГГ исковые требования Лосева И.В. удовлетворены частично. С ПАО «МТС» в пользу Лосева И.В. взысканы денежные средства за двойную оплату тарифов за январь 2016 год в размере 256 руб. 67 коп., за сентябрь 2016 года – 338 руб. 33 коп., штраф в размере 347 руб. 50 коп., компенсация морального вреда в размере 100 руб. В удовлетворении остальной части иска отказано. С ПАО «МТС» в доход бюджета города Смоленска взыскана государственная пошлина в размере 400 руб.

В апелляционной жалобе истец просит решение мирового судьи судебного участка №8 г. Смоленска от ДД.ММ.ГГГГ отменить, рассмотреть исковое заявление в Ленинском районном суде г.Смоленска ссылаясь на нарушение судом норм процессуального и материального права. В обоснование указывает, что суд не рассмотрел заявленные истцом исковые требования в части признания недействительными п.2 правил подписки на контент сайты adulvidos.ru, ozornica.com, playfullvideo.ru и п.8.5 Порядка предоставления контентных услуг МТС. Кроме того, указывает, что мировой судья в нарушение ст. 47 Конституции РФ отказал в удовлетворении его устного ходатайства о передаче дела на рассмотрение в Ленинский районный суд г.Смоленска к подсудности которого отнесено его рассмотрение. Полагает, что при рассмотрении дела мировой судья не применил п.1 ст. 16 Федерального закона от 07 февраля 1992 г. N 2300-1 "О защите прав потребителей", положения п.5 ст.54, п.5 ст.44, Федерального закона от 07.07.2003 №126-ФЗ «О связи». Указывает, что ответчиком в нарушение п.2 ст. 10 Федерального закона от 07 февраля 1992 г. N 2300-1 "О защите прав потребителей" не было предоставлено мировому судье доказательств предоставления абоненту информации о тарифах на услуги и кратком содержании данных услуг, а также о лице, предоставляющем конкретную услугу и лицевом счете с которого осуществляется списание денежных средств на оплату таких услуг в наглядной и доступной форме. Кроме того ссылается, что мировым судьей занижена сумма штрафа подлежащая взысканию в его пользу, как потребителя, поскольку в период рассмотрения спора ПАО «МТС» добровольно вернуло истцу 2 994 руб. 90 коп. Следовательно, с учетом указанной суммы должен быть рассчитан штраф.

В судебном заседании истец Лосев И.В. просил решение мирового судьи судебного участка №8 г. Смоленска от ДД.ММ.ГГГГ отменить по доводам, изложенным в апелляционной жалобе.

Представитель ответчика ПАО «МТС» Денисенков А.М. просил решение мирового судьи судебного участка №8 г. Смоленска от ДД.ММ.ГГГГ оставить без изменения, а апелляционную жалобу без удовлетворения, в обоснование привел доводы, изложенные ранее в письменном отзыве на иск.

Ответчик ООО «Стрим», надлежаще извещенное о дате и месте рассмотрения жалобы, в судебное заседание явку своего представителя не обеспечило.

В соответствии с ч.1 ст.327, ч.4 ст.167 ГПК РФ суд определил рассмотреть дело по существу в отсутствии не явившегося ответчика.

Заслушав доводы сторон, исследовав представленные доказательства, апелляционная инстанция приходит к следующим выводам.

В соответствии с ч.1 ст.330 ГПК РФ основаниями для отмены или изменения решения суда в апелляционном порядке являются: неправильное определение обстоятельств, имеющих значение для дела; недоказанность установленных судом первой инстанции обстоятельств, имеющих значение для дела; несоответствие выводов суда первой инстанции, изложенных в решении суда, обстоятельствам дела; нарушение или неправильное применение норм материального права или норм процессуального права.

Согласно ч.1 ст.327.1 ГПК РФ суд апелляционной инстанции рассматривает дело в пределах доводов, изложенных в апелляционных жалобе, представлении и возражениях

относительно жалобы, представления. Суд апелляционной инстанции оценивает имеющиеся в деле доказательства.

В силу ст. 79 ГК РФ по договору возмездного оказания услуг исполнитель обязуется по заданию заказчика оказать услуги (совершить определенные действия или осуществить определенную деятельность), а заказчик обязуется оплатить эти услуги. Правила настоящей главы применяются к договорам оказания услуг связи, медицинских, ветеринарных, аудиторских, консультационных, информационных услуг, услуг по обучению, туристическому обслуживанию и иных, за исключением услуг, оказываемых по договорам, предусмотренным главами 37, 38, 40, 41, 44, 45, 46, 47, 49, 51, 53 настоящего Кодекса.

Согласно ст. 781 ГК РФ заказчик обязан оплатить оказанные ему услуги в сроки и в порядке, которые указаны в договоре возмездного оказания услуг.

На основании ст. 782 ГК РФ заказчик вправе отказаться от исполнения договора возмездного оказания услуг при условии оплаты исполнителю фактически понесенных им расходов. Исполнитель вправе отказаться от исполнения обязательств по договору возмездного оказания услуг лишь при условии полного возмещения заказчику убытков.

В соответствии с п. 1 ст. 44 Федерального закона от 07.07.2003 года N 126-ФЗ "О связи", на территории Российской Федерации услуги связи оказываются операторами связи пользователям услугами связи на основании договора об оказании услуг связи, заключенного в соответствии с гражданским законодательством и правилами оказания услуг связи.

Согласно п. 2 ст. 44 Федерального закона от 07.07.2003 года N 126-ФЗ "О связи", Правила оказания услуг связи утверждаются Правительством Российской Федерации.

Правилами оказания услуг связи регламентируются взаимоотношения пользователей услугами связи и операторов связи при заключении и исполнении договора об оказании услуг связи, порядок идентификации пользователей услугами связи по передаче данных и предоставлению доступа к информационно-телекоммуникационной сети "Интернет" и используемого ими оконечного оборудования, а также порядок и основания приостановления оказания услуг связи по договору и расторжения такого договора, особенности оказания услуг связи, права и обязанности операторов связи и пользователей услугами связи, форма и порядок расчетов за оказанные услуги связи, порядок предъявления и рассмотрения жалоб, претензий пользователей услугами связи, ответственность сторон.

Постановлением Правительства РФ N 1342 от 09.12.2014 года утверждены правила оказания услуг телефонной связи.

В соответствии с п. 7 правил - оказания услуг подвижной связи, может сопровождаться предоставлением оператором связи иных услуг, технологически неразрывно связанных с услугами телефонной связи и направленных на повышение их потребительской ценности, при соблюдении требований, предусмотренных законодательными и иными нормативными правовыми актами Российской Федерации.

Перечень технологически неразрывно связанных с услугами связи иных услуг, направленных на повышение потребительской ценности услуг связи, которые оператор

связи имеет возможность предоставить абоненту и (или) пользователю, определяется оператором связи самостоятельно.

В соответствии с п. 24 правил, оказания услуг подвижной связи оператор связи обязан: оказывать абоненту и (или) пользователю услуги подвижной связи в соответствии с законодательными и иными нормативными правовыми актами Российской Федерации, настоящими Правилами, лицензией и договором; по требованию абонента или пользователя предоставлять дополнительную информацию, связанную с оказанием услуг подвижной связи.

В силу п. 2.19 Условий оказания услуг подвижной связи «МТС», услуги подвижной радиотелефонной связи, телематические услуги, услуги по передаче данных или иные сопряженные с ними услуги, оказываемые оператором непосредственно и /или с привлечением третьих лиц (сервисное, информационно-справочное обслуживание, услуги местной телефонной связи с представлением дополнительного абонентского номера без организации абонентской линии, конкретные услуги и др.).

Как установлено мировым судьей и подтверждается материалами дела, Лосев И.В. является абонентом ПАО «МТС», пользуется номером №.

С ДД.ММ.ГГГГ по ДД.ММ.ГГГГ Лосев И.В. пользовался тарифным планом «МТС Планшет». ДД.ММ.ГГГГ истец изменил тариф и по ДД.ММ.ГГГГ пользовался тарифным планом «Smart Nonstop». В период с ДД.ММ.ГГГГ по ДД.ММ.ГГГГ истец пользовался тарифным планом «Smart Безлимитище», который ДД.ММ.ГГГГ был изменен на тарифный план «МТС Коннект-4».

При использовании тарифного плана «Smart Nonstop» истцом ДД.ММ.ГГГГ в 18:40:18 была подключена услуга «МТС ТВ» с вариантом оплаты 15 руб./сутки. Условия оказания данной услуги доведены до абонентов на сайте оператора www.smolensk.mts.ru. Данная услуга отключена Лосевым И.В. ДД.ММ.ГГГГ. При этом, в период с апреля 2016 года по май 2017 года ответчиком произведено списание денежных средств в размере 6 360 руб.

ДД.ММ.ГГГГ в 13:48:10 истцом при использовании тарифного плана «Smart Безлимитище» была подключена услуга «Режим модема». При этом, в период с ноября 2016 года по май 2017 года ответчиком произведено списание денежных средств в размере 3 910 руб.

ДД.ММ.ГГГГ в 20:55:30 истец подключил мобильную подписку «http://playfullvideo.com» (код подписки №). Стоимость подписки составила 20 руб./сутки, контент-провайдер ООО «Стрим» с привлечением АО «Технолиния». ДД.ММ.ГГГГ в 20:08:30 абонент отключил подписку набором короткого USSD – запроса*152*22# для управления контентными подписками со своего мобильного телефона.

ДД.ММ.ГГГГ в 18:24:26 истцом была подключена мобильная подписка «http://ozornica.com» (код подписки №). Стоимость подписки составила 35 руб./2 дня, контент-провайдер ООО «Стрим» с привлечением ООО «Высокие технологии». ДД.ММ.ГГГГ в 7:31:23 абонент отключил подписку через приложение в личном кабинете.

ДД.ММ.ГГГГ в 21:17:41 Лосев И.В. подключил мобильную подписку «http://adultvidos.ru» (код подписки №). Стоимость подписки составила 20 руб./сутки, контент-провайдер ООО «Стрим» с привлечением ООО «МобиКит». ДД.ММ.ГГГГ в 7:31:21 абонент отключил подписку через приложение в личном кабинете.

ДД.ММ.ГГГГ истец обратился к ПАО «МТС» с письменной претензией содержащей требование о возврате излишне списанных денежных средств в сумме 14 998 руб. 90 коп., по результатам рассмотрения которой ответчик перечислил на счет Лосева И.В. 1700 руб.

Как следует из истории тарификации абонента № зафиксированы факты соединения абонентского номера истца с сервисными номерами (идентификатором услуги), отображающимися в детализации как №

Идентификатор № был выделен контент-провайдеру ООО «Высокие технологии», идентификатор № был выделен контент-провайдеру ООО «МобиКит» для оказания контентных услуг абонентам МТС на Интернет-сайте.

В период с января 2016 года по май 2017 года Лосеву И.В. были выставлены счета, в которых отражены факты соединения номер истца № с сервисными номерами. Начисления за контентные услуги в выставленных счетах отражаются как «Доступ к услугам контент-провадейров».

Как правильно отметил мировой судья основанием для списания ПАО «МТС» денежных средств со счета абонента № явилась активация кода доступа к подписке контент-провайдеров, что свидетельствует о том, что оферта контент-провайдера была акцептирована, свое согласие на оформление указанных выше мобильных подписок истец выразил.

Принимая решение, мировой судья руководствовался положениями ст. ст. 307, 309, 310, 779 ГК РФ, Федерального закона от 07 июля 2003 года № 126-ФЗ «О связи», Правилами оказания услуг подвижной связи, утвержденными Постановлением Правительства Российской Федерации от 25 мая 2005 года № 328, Условиями оказания услуг связи МТС, оценив по правилам ст. 67 ГПК РФ собранные по делу доказательства, пришел к выводу, что ответчиками соблюдены требования об информировании истца, перечень услуг определен абонентом согласно его тарифного плана и заказанной дополнительной услуги, в связи с чем, ПАО «МТС» обосновано списывались денежные средства со счета истца, за пользование подключенных услуг. Оснований для удовлетворения исковых требований в части взыскания денежных средств за не оказанную услугу «Подписка МТС ТВ» в размере 6 360 руб., денежных средств за не оказанную услугу «Режим модема» в размере 3 910 руб., денежных средств в размере 50% от суммы не оказанных услуг в размере 5 667 руб. 45 коп., денежных средств в размере 50% от суммы не оказанных услуг в размере 1340 руб. мировой судья не усмотрел.

С данными выводами мирового судьи суд апелляционной инстанции соглашается, поскольку они мотивированны, соответствуют обстоятельствам дела, содержанию исследованных судом доказательств и нормам материального права, подлежащим применению по настоящему делу.

Как верно установлено мировым судьей информация о тарифном плане, об услугах и стоимости подключения дополнительных услуг находится в открытом бесплатном доступе, на официальном сайте ПАО «МТС», а так же на сайте указанном при подключении

подписки на дополнительную услугу, необходимая информация о подключенных услугах и их стоимости предоставляется абоненту посредством набора коротких (сервисных) номеров, которые так же находятся в открытом доступе.

Доводы апелляционной жалобы о том, что ответчиком не представлено доказательств предоставления абоненту информации о тарифах на услуги и кратком содержании данных услуг, а также о лице, предоставляющем конкретную услугу и лицевом счете с которого осуществляется списание денежных средств на оплату таких услуг суд находит несостоятельными, поскольку они опровергаются письменными материалами дела и уже являлись предметом оценки и исследования судом первой инстанции.

В рамках рассмотрения спора мировым судьей разрешены все заявленные истцом, по уточненному исковому заявлению от ДД.ММ.ГГГГ, требования в части признания недействительными п.2 правил подписки на контент сайты adulvidos.ru, ozornica.com, playfullvideo.ru и п.8.5 Порядка предоставления контентных услуг МТС. Указанные требования были предметом изучения мирового судьи, мотивы их отклонения отражены в судебном акте, оснований не согласиться с ними у суда апелляционной инстанции не имеется.

Доводы апелляционной жалобы от том, что Лосев И.В. неоднократно заявлял мировому судье ходатайства о передаче дела на рассмотрение по подсудности в Ленинский районный суд г.Смоленска опровергаются протоколами судебных заседаний. Дело рассмотрено мировым судье в соответствии с установленными ст. 23 ГПК РФ правилами. Вывод истца о подсудности настоящего спора районному суду основан на неправильном толковании норм права.

Оценивая доводы приведенные Лосевым И.В. в апелляционной жалобе о занижении мировым судьей суммы штрафа, подлежащего взысканию в его пользу, суд апелляционной инстанции исходит из следующего.

В соответствии с ч.6 ст.13 Закона РФ «О защите прав потребителей» при удовлетворении судом требований потребителя, установленных законом, суд взыскивает с изготовителя (исполнителя, продавца, уполномоченной организации или уполномоченного индивидуального предпринимателя, импортера) за несоблюдение в добровольном порядке удовлетворения требований потребителя штраф в размере пятьдесят процентов от суммы, присужденной судом в пользу потребителя.

Поскольку денежные средства в сумме 2997 руб. 90 коп. были возвращены на счет истца ПАО «МТС» путем корректировки по лицевому счету в целях лояльности к абоненту, мировой судья верно определил размер штрафа в сумме 347 руб. 50 коп. (256,67+338,33+100), исходя из присужденной в пользу потребителя суммы.

Кроме того, суд отмечает, что добровольная выплата ПАО «МТС» суммы в размере 2 994 руб. 90 коп., в целях лояльности к абоненту, не свидетельствует об обоснованности заявленных исковых требований, от которых истец впоследствии отказался.

При таком положении, апелляционная инстанция находит принятое по делу судебное постановление законным и обоснованным, вынесенным в полном соответствии с нормами материального права, которые подлежали применению к спорным правоотношениям сторон, в связи с чем, не усматривает оснований к отмене данного судебного решения и удовлетворения апелляционной жалобы.

В целом, доводы апелляционной жалобы сводятся к изложению обстоятельств, являвшихся предметом исследования и оценки суда первой инстанции и к выражению несогласия с произведенной судом оценкой представленных по делу доказательств.

Каких-либо иных нарушений, в том числе процессуального характера, являющихся безусловным основанием для отмены судебного акта суд, апелляционной инстанции не усматривает.

Руководствуясь ст.ст.328-330 ГПК РФ, суд

о п р е д е л и л:

Решение мирового судьи судебного участка № 8 в г. Смоленске от 24.04.2018 оставить без изменения, а апелляционную жалобу Лосева Игоря Владимировича - без удовлетворения.

Апелляционное определение вступает в законную силу со дня его принятия.

Судья В.В. Манаков

Мотивированное апелляционное определение изготовлено 16.07.2018

- **Дело №2-225/2018**

Номер дела: 2-225/2018

Дата начала: 25 августа 2017 г.

Дата рассмотрения: 27 марта 2018 г.

Суд: Центральный районный суд г. Новосибирск

Судья: Малахов Сергей Леонидович

Решение

27 марта 2018 года

Центральный районный суд г. Новосибирска в составе:

судьи С.Л. Малахова,

при секретаре К.С. Кулаковой

рассмотрев в открытом судебном заседании гражданское дело по иску Майснер ххх к Обществу с ограниченной ответственностью «Т2 Мобайл» о взыскании денежных средств,

у с т а н о в и л:

Майснер Л.А. обратилась в суд с иском к ООО «Т2 Мобайл», просит взыскать в ответчика сумму неосновательного обогащения в размере 53715 рублей 56 копеек, проценты за пользование чужими денежными средствами в размере 4938 рублей 11 копеек и по дату фактического исполнения решения суда, компенсацию морального вреда в размере 10000 рублей, расходы по оказанию юридической помощи в размере 20000 рублей, штраф в размере 50 % за неудовлетворение ответчиком требований истца в добровольном порядке, в связи с неправомерным взысканием ответчиком платы за услуги, подключенной без согласия абонента.

Истец Майснер Л.А., ее представитель Кыймаштаев А.В., действующий на основании доверенности, в судебном заседании заявленные исковые требования поддержали в полном объеме, дали соответствующие пояснения.

Представитель ответчика ООО «Т2 Мобайл» Федорова Д.К., действующая на основании доверенности, в судебном заседании заявленные исковые требования не признала в полном объеме по основаниям, изложенным в письменных возражениях, дала соответствующие пояснения.

Выслушав мнение лиц, участвующих в деле, исследовав собранные по делу доказательства, суд приходит к выводу об отказе в удовлетворении заявленных требований, при этом исходя из следующего.

В соответствии с положениями статьи 8 Гражданского кодекса РФ гражданские права и обязанности возникают из оснований, предусмотренных законом и иными правовыми актами, а также из действий граждан и юридических лиц, которые хотя и не предусмотрены законом или такими актами, но в силу общих начал и смысла гражданского законодательства порождают гражданские права и обязанности.

В соответствии с этим гражданские права и обязанности возникают, в частности, из договоров и иных сделок, предусмотренных законом, а также из договоров и иных сделок, хотя и не предусмотренных законом, но не противоречащих ему; в результате приобретения имущества по основаниям, допускаемым законом.

В соответствии с пунктом 1 статьи 420 Гражданского кодекса РФ договором признается соглашение двух или нескольких лиц об установлении, изменении или прекращении гражданских прав и обязанностей.

Согласно пункту 1 статьи 432 Гражданского кодекса РФ договор считается заключенным, если между сторонами, в требуемой в подлежащих случаях форме, достигнуто соглашение по всем существенным условиям договора.

В соответствии со статьей 309 Гражданского кодекса РФ обязательства должны исполняться надлежащим образом.

Согласно статье 310 Гражданского кодекса РФ односторонний отказ от исполнения обязательств и одностороннее изменение его условий не допускаются, за исключением случаев, предусмотренных законом.

Согласно преамбуле ФЗ "О связи", указанный Закон устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

В силу статьи 44 Федерального закона "О связи", на территории Российской Федерации услуги связи оказываются операторами связи пользователям услугами связи на основании договора об оказании услуг связи, заключенного в соответствии с гражданским законодательством и правилами оказания услуг связи.

Правила оказания услуг связи утверждаются Правительством Российской Федерации.

Правилами оказания услуг связи регламентируются взаимоотношения пользователей услугами связи и операторов связи при заключении и исполнении договора об оказании услуг связи, порядок идентификации пользователей услугами связи по передаче данных и предоставлению доступа к информационно-телекоммуникационной сети "Интернет" и используемого ими оконечного оборудования, а также порядок и основания приостановления оказания услуг связи по договору и расторжения такого договора, особенности оказания услуг связи, права и обязанности операторов связи и пользователей услугами связи, форма и порядок расчетов за оказанные услуги связи, порядок предъявления и рассмотрения жалоб, претензий пользователей услугами связи, ответственность сторон.

В соответствии со статьей 46 указанного Федерального закона, оператор связи обязан оказывать пользователям услугами связи услуги связи в соответствии с законодательством Российской Федерации, техническими нормами и правилами, лицензией, а также договором об оказании услуг связи.

Судебным разбирательством установлено, что между Майснер Л.А. и ООО «Т2 Мобайл» 27.06.2014 года заключены договоры об оказании услуг подвижной радиотелефонной связи с использованием телефонных номеров: +7953ххх; +7953ххх; +7953ххх; +7953ххх.

Как указывает истец в своем иске, в период с 01.03.2016 года по 01.03.2017 года с лицевых счетов истца ООО «Т2 Мобайл» были списаны денежные средства в общей сумме 53715 рублей 56 копеек:

- с номера +7953ххх сумма в размере 16658 рублей 70 копеек;

- с номера +7953ххх сумма в размере 5338 рублей 93 копейки;

- с номера +7953ххх сумма в размере 22145 рублей 47 копеек;

- с номера+7953ххх сумма в размере 9572 рубля 48 копеек.

Указанное подтверждается представленной в материалы дела выпиской по лицевому счету. Списание денежных средств в указанном размере ответчиком в судебном заседании не оспаривалось.

Между тем, как указывает истец, денежные средства в общей сумме 53715 рублей 56 копеек были списаны ответчиком за услугу «заказ контента», однако истец данный вид услуги не заказывала, согласия оператору связи на подключение дополнительных услуг не давала, в устройстве Asteroid, используемой истцом в качестве для одновременного подключения четырех сим-карты с указанными номерами, отсутствует возможность для отправки СМС-сообщений для подключения контентов.

Полагая, что ответчик незаконно удержал денежные средства истца в общей сумме 53715 рублей 56 копеек, что привело к неосновательному обогащению, обратилась в суд с настоящим иском.

Отказывая истцу в удовлетворении заявленных исковых требований, суд исходит из следующего.

Как следует из пояснений истца, все 4 сим-карты с номерами +7953ххх; +7953ххх; +7953ххх; +7953ххх использовались одновременно в одном устройстве Asteroid (серийный номер 2456790B0188).

IMEI портов названного устройства: 3554570521080133; 355457052180240; 355457052180208; 355457052180281 совпадают с IMEI оборудовании, работающего с вышеуказанными номерами, что подтверждается сведениями из ответа ООО «Теле2» на запрос суда.

Согласно абзацу 34.1 статьи 2 Федерального закона «О связи» контентные услуги - вид услуг связи, которые технологически неразрывно связаны с услугами подвижной радиотелефонной связи и направлены на повышение их потребительской ценности (в том числе услуги по предоставлению абонентам возможности получать на пользовательское (оконечное) оборудование в сетях связи справочную, развлекательную и (или) иную дополнительно оплачиваемую информацию, участвовать в голосовании, играх, конкурсах и аналогичных мероприятиях) и стоимость оказания которых оплачивается абонентом оператору связи, с которым у абонента заключен договор об оказании услуг связи;

В соответствии с абзацами 2,3 части 5 названного Федерального закона оказание иных услуг, технологически неразрывно связанных с услугами подвижной радиотелефонной связи и направленных на повышение их потребительской ценности, осуществляется с согласия абонента, выраженного посредством совершения им действий, однозначно идентифицирующих абонента и позволяющих достоверно установить его волеизъявление на получение данных услуг.

До получения согласия абонента об оказании иных услуг связи, технологически неразрывно связанных с услугами подвижной радиотелефонной связи и направленных на повышение их потребительской ценности, в том числе контентных услуг, оператор связи должен предоставлять абоненту информацию о тарифах на услуги и кратком содержании данных услуг, а также о лице, предоставляющем конкретную услугу, и лицевом счете, с которого осуществляется списание денежных средств на оплату таких услуг. Расчеты за оказанные абоненту услуги осуществляются оператором связи.

Операторы связи несут ответственность перед абонентами за нарушение требований, установленных пунктом 5 статьи 44 названного Федерального закона, при подключении и предоставлении иных услуг связи, технологически неразрывно связанных с услугами подвижной радиотелефонной связи и направленных на повышение их потребительской ценности, в том числе контентных услуг.

Согласно представленных данных программно-аппаратного комплекса ООО «А1Системс» с абонентских номеров +7953ххх; +7953ххх; +7953ххх; +7953ххх, посредством интерактивных тизеров, были сделаны запросы на подключение контента, при этом, тизеры содержали в себе информацию о полной стоимости услуги (сервиса), запрос на подтверждение согласия абонента на ее активацию, при этом, суд учитывает, что для получения согласия на активацию контента абоненту необходимо совершить самостоятельное физическое действие по нажатию на соответствующую «иконку» на дисплее телефона (принять/отменить), только после нажатия абонентом варианта ответа «принять» контент будет подключен оператором, о чем на телефон абонента придет соответствующее сообщение.

Как следует из представленных в материалы дела детализаций используемых истцом номеров, с последних неоднократно направлялись заказы контента, то есть согласие абонента на подключение услуги в ответ на приходящие абоненту сообщения о запросе контента.

Сама по себе детализация предоставленных услуг является относимым и допустимым доказательством получения абонентом запроса контента, последующего заказа контента и его стоимости.

Каких-либо доказательств опровергающих сведения о заказе абонентом контента либо доказательств навязывания в подключении контентов абоненту в одностороннем в отсутствии согласия абонента оператором связи, истцом в материалы дела не представлены.

При этом, контент-услуги, согласно указанным детализациям предоставленных услуг использовались абонентом с номеров +7953ххх; +7953ххх; +7953ххх; +7953ххх в период с 22.03.2016 года по 14.03.2017 года.

Помимо прочего, как следует из детализации подписок (л.д. 99-105) истец не только подключала подписки, но и самостоятельно их отключала, из чего суд приходит к выводу о том, что истец ознакомлена с процедурой включения/отключения подписок.

Согласно выписке по лицевым счетам указанных номеров, за вышеназванный период истцом регулярно вносилась оплата на общую сумму 53715 рублей 56 копеек:

Так, согласно представленным детализациям за указанный период:

- с номера +7953ххх списана сумма в размере 16658 рублей 70 копеек;

- с номера +7953ххх списана сумма в размере 5338 рублей 93 копейки;

- с номера +7953ххх списана сумма в размере 22145 рублей 47 копеек;

- с номера+7953ххх списана сумма в размере 9572 рубля 48 копеек.

Данные суммы являются значительными и истец, при проявлении надлежащей заботливости и осмотрительности, не могла не заметить существенного увеличения расходов на мобильную связь, однако доказательств обращения к ответчику в спорный период с соответствующими заявлениями в материалах дела не имеется.

Доводы истца о том, что устройство Asteroid (серийный номер 2456790B0188), используемое истцом для всех четырех сим-карт одновременно, не предназначено для передачи СМС-сообщений судом не принимаются, поскольку опровергается представленными фактами использования абонентом услуг и ответом на запрос суда о IMEI оборудования, работающего с номерами истца, с которых осуществлялись запросы и заказы услуг.

Ссылки истца на письмо производителя оборудования Asteroid ООО «Парабел» об отсутствии возможности приема и передачи СМС сообщений в программном обеспечении шлюза, не свидетельствует, что конкретное устройство истца не имело физического вмешательства для обновления либо изменения программного обеспечения, по результату которого данная функция была изменена и возникла вероятность, в том числе и помимо воли истца возможность приема и отправки различного рода сообщений, в частности в ответ на запрос услуги подключаться к ней в автоматическом режиме.

Относимых и допустимых доказательств обратного истцом, вопреки требованиям статьи 56 Гражданского процессуального кодекса РФ, суду не представлено, ходатайств о назначении судебной экспертизы для подтверждения своих доводов, истом суду не заявлялось.

На основании изложенного, суд приходит к выводу об отсутствии правовых оснований для удовлетворения требования истца о признании полученных ответчиком денежных средств в общей сумме 53715 рублей 56 копеек неосновательным обогащением и взысканием указанной суммы в пользу истца.

Кроме того, не подлежат удовлетворению требования истца о взыскании процентов, компенсации морального вреда, судебных расходов, штрафа, поскольку данные требования являются производными от основного требования, а в удовлетворении основного требования истцу судом отказано.

На основании вышеизложенного и руководствуясь статьями 194-198 Гражданского процессуального кодекса Российской Федерации, суд

р е ш и л:

Исковые требования Майснер ххх – оставить без удовлетворения.

Разъяснить сторонам, что настоящее решение может быть обжаловано ими в течение месяца со дня принятия решения судом в окончательной форме в Новосибирский областной суд путем подачи апелляционной жалобы через суд, вынесший решение.

Мотивированное решение изготовлено 06 апреля 2018 года

Судья С.Л. Малахов

6.2. Обзоры и оценки экспертов, средств массовой информации, блогеров о перспективах развития рынка

- **Ведомости – Где сотовые операторы ищут новые источники доходов**
  https://www.vedomosti.ru/technology/articles/2018/03/21/754381-sotovie-operatori-istochniki

«Падение доходов от звонков и sms заставляет их предлагать абонентам все новые услуги

В середине 2000-х гг. доходы российских операторов от их традиционных услуг вроде телефонных звонков или отправки sms ежегодно росли более чем на 30%. Но после кризиса 2008–2009 гг. рост сначала резко замедлился, а с 2014 г. прекратился и даже стал показывать отрицательную динамику, следует из данных AC&M Consulting. Мобильные услуги все еще приносят операторам львиную долю денег, но, поскольку доходы от мобильной связи как минимум не растут, операторы ищут для себя новые направления бизнеса, отмечает аналитик Райффайзенбанка Сергей Либин.

Теперь основные надежды операторы возлагают на новые и непривычные для телекоммуникаций бизнесы – от мобильного ТВ и музыкальных сервисов до интернета вещей и системной интеграции. Сейчас новые сервисы уже приносят МТС до 20% выручки, говорил на бизнес-ужине «Ведомостей» на Mobile World Congress член правления МТС Вячеслав Николаев. В 2018 г. оператор успел отметиться несколькими неожиданными сделками: в феврале купил известные онлайн-сервисы по продаже билетов Ticketland и

Ponominalu.ru, а в середине января – киберспортивный клуб Gambit Esports. МТС назвала покупки «еще одним шагом за пределы традиционного телекома». И МТС не единственная, кто опасается остаться всего лишь трубой для перекачки контента. В 2017 г. все российские операторы представили стратегии цифрового развития, которые во многом схожи: они предусматривают развитие финансовых услуг, использование больших данных, системную интеграцию, интернет вещей и электронную коммерцию.

Бонусные программы, цифровое телевидение и музыка

В прошлом году российская большая тройка сотовых операторов предприняла попытку «ремонта рынка» – отказалась от ценовой конкуренции в пользу продажи большего количества услуг абонентам за большие деньги, напоминает гендиректор «ТМТ консалтинга» Константин Анкилов.

«Мегафон» уходит от понятия «оператор связи» и фокусируется на увеличении времени, которое абонент проводит в сети, за счет различных цифровых сервисов, говорит представитель оператора Юлия Дорохина. МТСпланирует внедрять IT-технологии во все продукты, сервисы и свою операционную деятельность, объявив диджитализацию одним из ключевых пунктов собственной стратегии. Tele2 предложила пользователям бонусные программы (например, в сервисе такси Gett) и различные digital-сервисы в партнерстве с другими компаниями. «Мы все, как операторы, мечтаем в конечном итоге стать немножко «Тинькофф банком», когда между нами и абонентом будет только цифровой интерфейс», – сказал в июне 2017 г. на конференции «Ведомостей» заместитель генерального директора по продукту, маркетингу и работе с федеральными клиентами Tele2 Андрей Патока. Дополнительные сервисы интересны и самим абонентам: согласно февральскому исследованию EY даже больше связи абонентам за пределами Москвы интересны банковские услуги (39,5% опрошенных), системы безопасности дома и автомобиля (38 и 36%) и геолокация членов семьи (47%).

Уже несколько лет доходы операторов от услуг голосовой связи отбирают OTT-сервисы (в них передача контента происходит «поверх» сетей операторов связи, так работают мессенджеры и онлайн-кинотеатры), отмечает Анкилов. Это обстоятельство подтолкнуло операторов к созданию собственных продуктов такого рода: «МТС Connect», мессенджер «Мегафона» «Мультифон», в 2016 г. переименованный в eMotion, платформа «Вымпелкома» Veon. Последняя, по данным самой компании, за 2017 г. получила 1,7 млн регистраций в России и помимо сообщений дает клиентам льготный доступ к предложениям партнеров (сервисы такси, доставка еды и др.). Но отобрать пальму первенства у WhatsApp, Viber и Telegram до сих пор не удалось, свидетельствуют данные MediaScope.

У всех операторов есть собственные предложения цифрового ТВ, которые они развивают самостоятельно или в партнерстве с онлайн-кинотеатрами (такими, как «Амедиатека», Megogo и др.). Также все они предлагают специальные сервисы для любителей музыки. Сколько эти сервисы приносят денег, операторы не раскрывают, но представитель «Мегафона» говорит, что общее число абонентов «Мегафон.ТВ» выросло в 3 раза за год до 3 млн на конец 2017 г. (число активных и платящих подписчиков оператор не раскрывает), а доходы – в 1,5 раза.

Еще одним сервисом для удержания клиентов в сети должны стать удаленные консультации с врачами. Первым такую услугу в ноябре прошлого года предоставил «Мегафон» – сервис «Мегафон.Здоровье». Аналогичные проекты сейчас тестирует МТС, «Билайн» ищет партнера для запуска, сообщили их представители. «Ростелеком» с 2016 г. разрабатывает систему дистанционных медицинских консультаций, но его представитель не смог ответить на вопрос, когда планируется ее запуск.

Финансовые сервисы и мобильные платежи

У всех операторов есть и финансовые сервисы. Например, они предлагают абонентам банковские карты с кэшбэком: Tele2 предлагает абонентам хранить деньги прямо на счете мобильного телефона – доходность составляет 5% годовых. «Вымпелком» и МТС запустили в 2017 г. микрокредитование. Разумеется, все операторы предлагают использовать номер телефона для оплаты услуг.

Зарабатывают операторы и на страховании – совместно с партнерами предлагают услуги от страхования техники (есть у всех операторов) до недвижимости («Вымпелком» и Tele2) и автострахования (МТС). Выручка от страховок «Вымпелкома» за III квартал 2017 г. выросла в 5 раз год к году, говорит представитель оператора Анна Айбашева, а представитель «Мегафона» указывает, что финансовые услуги в салонах выросли в объеме за последний год более чем в 2 раза.

Рынок финансовых услуг интересен всем федеральным игрокам. Но возможности мобильных платежей с использованием операторского счета ограничивает конкуренция с традиционным и мобильным банкингом, говорит Анкилов. По оценкам «ТМТ консалтинга», проникновение финансовых услуг в абонентскую базу сотовых операторов в 2017 г. составило лишь 5%. По оценкам AC&M Consulting, общий оборот рынка мобильных финансовых услуг в 2016 г. составил 87 млрд руб. (рост на 25% к 2015 г.), а число пользователей выросло на 15% до 13,7 млн человек.

Интернет вещей

Одним из главных направлений для роста мобильных операторов должен стать рынок интернета вещей (IoT). Он включает в себя мониторинг устройств в доме, систем безопасности, управления городской инфраструктурой, ЖКХ и промышленными предприятиям – устройства и датчики подключаются к интернету, и специальные системы анализируют ненужные клиенту процессы и в случае необходимости управляют ими. База мобильных абонентов в России уже не вырастет, а вот количество сим-карт для подключения автоматических устройств (так называемые m2m) за четыре года удвоится, прогнозирует Анкилов. В 2017 г. число таких устройств в России составило 15 млн, отмечает он.

По данным AC&M Consulting, лидером по итогам первого полугодия 2017 г. по количеству подключенных устройств является МТС (на нее приходилось 42% m2m-карт), на 2-м месте – «Мегафон» (36%), на 3-м – «Вымпелком» (18%). МТС развивает свои IoT-решения с помощью купленного в 2015 г. системного интегратора NVision Group и на конец первого полугодия оператор обслуживал 4,5 млн m2m-устройств, говорит представитель МТС. В декабре прошлого года МТС открыла платформу для промышленного IoT и предоставила клиентам услугу «Телеучет данных», которую компании могут использовать в производстве и сельском хозяйстве, логистике, коммерческой недвижимости и других

сферах. «Вымпелком» предоставляет IoT-решения на базе собственной платформы «Единый мониторинг», которая объединяет датчики, трекеры, смартфоны и планшеты в единую экосистему, сообщил представитель оператора. В будущем он планирует создавать на ней решения для ЖКХ, энергетики и систем умного города.

Представитель «Мегафона» настаивает, что доля оператора на рынке умных устройств составляет 37%. Решения оператора используются для автоматизированного мониторинга ресурсов ЖКХ в татарстанском Иннополисе, оператор внедряет умное городское освещение в Брянске, а в Челябинске – дорожные знаки, перечисляет его представитель Юлия Дорохина. Помимо этого с 2016 г. «Мегафон» предлагает своим клиентам купить систему умного дома Life Control – она представляет собой набор датчиков электроэнергии, дыма, открытия и закрытия дверей. Система домашнего видеонаблюдения есть и у «Ростелекома».

Для операторов интернет вещей – это возможность зарабатывать как на передаче данных, так и на самих устройствах и их обслуживании, отмечает Анкилов. Например, «Ростелеком» заработал в 2016 г. на различных проектах умного города – от городских транспортных систем до систем электронного образования – 7,2 млрд руб. (на 68% больше, чем годом ранее)».

- **Forbes – Не только разговоры: как будут развиваться мобильные операторы**
  http://www.forbes.ru/biznes/359659-ne-tolko-razgovory-kak-budut-razvivatsya-mobilnye-operatory

«Пытаясь переломить тенденцию превращения мобильного оператора в трубу для доставки контента, крупнейшие мировые игроки начали борьбу за абонентов, предлагая им все новые и новые цифровые сервисы

В марте мобильные операторы подвели финансовые итоги своей деятельности за 2017 год. Это был первый год за последние пять лет, когда мы смогли наблюдать рост прибыльности в абсолютном выражении. МТС увеличил выручку практически на 12 млрд рублей, а «Мегафон» и «Билайн» на 5,5 и 2,8 млрд рублей соответственно. Разворота удалось достичь благодаря тому, что в начале 2017 года операторы начали «ремонт рынка». Компании перестали демпинговать и гнаться за количеством проданных сим-карт, а вместо этого переключились на удержание абонентов. К концу года хрупкое перемирие было нарушено, и телеком-компании вернулись к ценовым войнам в некоторых регионах. Это негативно скажется на финансовых показателях в 2018 году. Оздоровление показателей также стало возможным благодаря тому, что крупнейший игрок на рынке сотовой связи, компания МТС, перестал наращивать свою розничную сеть, сократив сопутствующие маркетинговые акции по ее продвижению. Удалось ли мобильным операторам переломить негативный тренд или это лишь временное явление, которое так и не оформится в тенденцию?

То, что классические услуги по передаче голосовых данных и трафика не могут обеспечивать рост выручки, сегодня очевидно всем. Трафика с каждым годом становится все больше, себестоимость его передачи растет, а выручка и прибыльность от оказания этого типа услуг только падает. Пытаясь переломить тенденцию превращения мобильного оператора в трубу для доставки контента, крупнейшие мировые игроки начали борьбу за абонентов, предлагая им все новые и новые цифровые сервисы.

Объединение с медиабизнесом

Одна из главных тенденций последних двух лет – объединение мобильных операторов с медиабизнесом. Производителям контента нужен доступ к смартфонам, новым каналам распространения, которым отдает предпочтение молодая аудитория, а телеком-компаниям нужен контент, чтобы повышать лояльность своих клиентов и зарабатывать на новых сервисах. Так, например, американская AT&T уже второй год добивается разрешения на покупку крупнейшего медиахолдинга Time Warner за $85 млрд, Verizon заканчивает приобретение интернет-медиабизнеса Yahoo, а T-Mobile рассматривает покупку Dish Network. Еще в 2016 году российские операторы также делали смелые заявления о намерении распространять видеоконтент, но ограничились безопасными и ничем не примечательными партнерствами с онлайн-кинотеатрами. Осторожные инвестиции ожидаемо обернулись минимальными результатами.

В 2017 году представители телеком-отрасли в России начали более активно инвестировать в новые бизнесы: «Мегафон» получил контроль над Mail.ru Group, «Билайн» запустил и активно продвигал платформу VEON (симбиоз мессенджера и агрегатора онлайн-сервисов), а МТС инвестировал в ряд инновационных компаний. Эти приобретения могли бы позволить операторам более глубоко изучить своих клиентов, предложить им нестандартные услуги и заняться цифровизацией взаимоотношений с абонентами, сократив расходы на отдельные направления работы с ними. Но в прошлом году мы так и не увидели ни одного совместного проекта «Мегафона» и Mail.ru Group, а платформе VEON, у которой, по данным Mediascope, 750 000 активных пользователей, еще очень далеко до реальной конкуренции с мессенджерами WhatsApp и Telegram, у которых 22 и 7,3 млн пользователей соответственно.

Не менее скромные результаты и в том, что касается сервисов, основанных на больших данных, притом, что операторам доступна информация о демографии, геолокации, уровне дохода, контактах и особенностях использования мобильного интернета, которую они бережно хранят, но не используют в полную силу. Существующие на российском рынке кейсы освоения больших данных телеком-компаниями в основном были связаны с удержанием клиентов, оценкой прибыльности абонентов, созданием индивидуальных тарифов и оптимизацией бизнес-процессов, т. е. направлены на сокращение расходов, а не на получение дополнительной прибыли от новых продуктов.

Одна из причин медленного развития представителей отрасли в альтернативных направлениях – их консервативный подход к ведению бизнеса и банальная инерция. Справиться с проблемой помогут более расторопные союзники. Для мобильных операторов такими партнерами могут стать интернет-компании. Эти сегменты не являются конкурирующими, как может показаться на первый взгляд. Предоставление доступа в интернет в любом случае останется за телекомом. Опыт интернет-компаний в оперативной разработке и запуске продуктов даст возможность телеком-компаниям прийти к новой модели монетизации. А интернет-гиганты, в свою очередь, получат доступ к еще большему количеству данных о пользователях. Проверить эту теорию можно будет уже в этом году, если произойдет анонсированная ранее синергия «Мегафона» и Mail.ru Group.

Рекомендательные сервисы и интернет вещей

Один из сценариев, по которому могли бы развиваться такие продукты, является направление рекомендательных сервисов. Мобильные операторы могут взять на себя функцию консьержа или личного помощника, предложив пользователю подходящие услуги, товары и контент на основании собственной и партнерской информации. Первый шаг в этом направлении сделала компания МТС, закрывшая в феврале сделку по приобретению билетных операторов Ticketland.ru и «Пономиналу». На эти сервисы приходится четверть российского рынка продажи билетов на концерты, театральные постановки и спортивные мероприятия. Интеграция имеющихся у оператора данных с информацией, полученной от платформ, позволит предложить клиентам билеты со скидками по программе лояльности.

Безусловно перспективное для телекома направление – интернет вещей. За последние 10 лет в России было продано более 1,1 млрд SIM-карт, а число действующих абонентов превысило 250 млн человек. При этом население страны осталось на отметке 146 млн человек. Очевидно, что массовых новых подключений ожидать не стоит. Но это не относится к M2M-соединениям – то есть межмашинным взаимодействиям, во время которых устройства обмениваются интернет-сигналами между собой. По оценкам GSMA, к 2020 году их количество в России превысит 26 млн.

К сожалению, из-за низкой стоимости услуг связи для IoT мобильные операторы смогут извлечь прибыль только в краткосрочной перспективе. Чтобы занять прочные позиции на рынке интернета вещей, телеком-компаниям необходимо уже сегодня задуматься о развитии собственных сервисов. Например, не просто дать умным устройствам доступ в интернет, но и обеспечить пользователей полным набором инструментов по их контролю, таких как управление SIM-картами, операционная и аналитическая отчетность, контроль баланса, диагностика качества сети, контроль смены устройства, местоположение устройства по информации базовых станций.

Еще один шаг к успеху на рынке IoT – это разработка собственных IT-решений, платформ и приложений, которые позволят объединять сторонние устройства и оперативно интегрироваться с партнерами. В этом направлении уже работает «Мегафон», запустивший в 2016 году линейку устройств для умного дома под брендом Life Control, которые представляют из себя единую экосистему.

Более масштабное, но и гораздо более сложное развитие ждет индустриальный интернет вещей. Для успешной работы тут не достаточно одного желания мобильных операторов отвоевать кусок рынка. Здесь необходима синергия усилий государства и бизнеса, их готовность экспериментировать и развивать новую экосистему. Более того, необходимо, чтобы бизнес пришел к осознанию необходимости и экономической привлекательности индустриального интернета вещей. На текущий момент в России уже есть пионеры отрасли, но нам необходимо совместными усилиями делать это направление массовым.

Сейчас российские телеком-компании уже поняли, что традиционный бизнес не сможет обеспечить уровень прибыльности, на котором настаивают акционеры. Перед операторами открыто много дверей, но сегодня становится важно не только то, что они собираются трансформировать, но и то, как это будет сделано. Для того чтобы не остаться в прошлом и не кануть в лету, телеком-компаниям необходимо идти в ногу со временем, быстро меняющимся миром и растущими требованиями клиентов. Операторам нужен

новый взгляд на такие аспекты бизнеса, как инвестиционные кейсы в новой экономике, борьба за таланты, борьба за новых и удержание старых абонентов. Им необходимо изменить и сам подход к управлению приобретаемыми активами.

Схема, когда приобретенный бизнес переделывался по существующим лекалам, устарела вместе с этими самыми лекалами. Активы в области инноваций требуют осторожного отношения – необходимо присмотреться к тому, как функционирует бизнес, заимствовать лучшее, при этом не нарушив хрупкую экосистему и не убив предпринимательский дух. Более того, сегодня, в эпоху share economy, не нужно непременно владеть бизнесом. Подчас продуктивнее будет создавать взаимовыгодные партнерства операторов с различными компаниями».

- **Forbes – Мобильные операторы ищут новые источники дохода**
  https://www.rbc.ru/society/05/06/2008/5703ccea9a79470eaf76b00b

«Поиск дополнительных доходов вынуждает мобильных операторов менять свой контент, предлагая дополнительные услуги в сегменте широкополосного интернет-доступа (ШПД).

"Так, уже сегодня 50% населения по утрам просматривает прогноз погоды на своих мобильных, а 30% - новости", - отмечает в гостях у программы "В фокусе" на РБК-ТВ генеральный директор компании "Дейтариум" Дмитрий Комиссаров. "За последний год трафик в сети поднялся в 6-7 раз, и мы ожидаем, что не менее половины доходов компании будет связано с мобильной передачей данных или с мобильным Интернетом", - рассказывает заместитель генерального директора ЗАО "Скай Линк" Альберт Сафиуллин.

Мобильные операторы уверены, что в перспективе, по мере продвижения в массы дешевых и удобных мобильных устройств, совмещенных с широкополосным доступом, появятся приложениям и сервисы, которые пользуются популярностью на iPhone (совмещающий в себе мобильный телефон, цифровой плеер, Интернет), а также те, о которых пока ничего не известно. Например, электронная книга будут использовать мобильную передачу данных для закачки новых книг. Через три года каждый телефонный аппарат будет похож на iPhone с широкополосным доступом 3G, через четыре года каждое устройство будет оборудовано GPS-навигатором. Но самое главное, что эти устройства будут оснащены интерфейсом, удобным и понятным практически любому пользователю, отмечает Д.Комиссаров.

Правда, генеральный директор "Дымшиц и партнеры" Михаил Дымшиц уверен, что количество людей, которым нужно узнать погоду, курсы валют, ситуацию на дорогах, ограничено, поскольку большей части населения эти сервисы не нужны по жизни. Люди пользуются большим количеством приложений из любопытства, а наигравшись в мелодии и картинки, вновь приоритетной остается функция "говорить".

Правда, однозначно сказать, какие услуги будут пользоваться популярностью у населения, тоже невозможно. Это из серии "удивительное рядом", говорит Д.Комиссаров. Например, в Европе выжимки тревел-гайдов (туристический справочник) составляют треть продаж, которые загружаются на iPod. Правда, и цены на услуги сотовых операторов должны быть приемлемыми. В Европе видеозвонки не настолько популярны, как в Корее и Японии, по одной простой причине: это дорого. "Никто не будет звонить за три доллара с видеорежимом и грузить фильм по за шесть-восемь долларов", - резюмирует он.

Надо сказать, что крупнейший оператор МТС, впрочем, как и другие отечественные операторы сотовой связи, провели ребрендинг, дабы сделать их услуги более востребованными. Правда, по оценке М.Дымшица, ребрендинг "Билайна" и МТС следует признать неэффективным, если количество абонентов и доля на рынке в денежном выражении падает. Понятно, что эти операторы росли, увеличивая свое присутствие на рынке за счет слияний и поглощений в России и за рубежом, тогда как на московском рынке на фоне ребрендинга и те, и другие потеряли свою долю на рынке, подытожил он».

- **Habr – Цифровая трансформация телекома, или как операторы «идут» в ИТ**
  https://habr.com/ru/company/comptek/blog/353870/

В статье по этой ссылке представлен прогноз возможного развития и трансформации операторов связи.

- **VC.RU – Будущее мобильных приложений в ближайшие 10 лет**
  https://vc.ru/flood/43819-budushchee-mobilnyh-prilozheniy-v-blizhayshie-10-let

«К 2025-му году услугами мобильной индустрии будет пользоваться 5,9 млрд уникальных мобильных абонентов, или 71% ожидаемого населения Земли

У современного пользователя смартфона в среднем установлено в устройстве 35 мобильных приложений. Однако многие из них удаляются после первого использования. Часто это связано с плохой работоспособностью или низкой производительностью. При этом мобильная индустрия продолжает развиваться и количество мобайл-стартапов только растет.

Я проанализировал зарубежную аналитику и мнение ведущих IT-компаний. Итак, что ждет рынок мобайла в течение следующего десятилетия? Полагаю, что мы увидим, как развивается связка искусственного интеллекта с потребностями пользователей. Это должно сблизить пользователя с его мобильным устройством.

Какие перспективы у приложений с потоковым контентом и голосовым управлением?

По мере того, как технология 5G уже подступает к производителям гаджетов, способность передачи и загрузки видеоконтента будет стремительно расти. Этому способствует и экспоненциальное развитие самого контента, благодаря социальным сетям.

Поскольку Siri и Google Assistant уже достигли своего потенциала, в ближайшее время мы увидим повсеместное внедрение голосового управления. Это откроет больше возможностей как для «издательских» приложений, так и для маркетологов для более тесного общения со своими потребителями.

Куда все движется?

Будущее приложений можно разделить на три основных блока.

Скорость и эффективность: среда мобильных приложений работает быстрее по сравнению с мобильной сетью. Эта скорость позволяет пользователям быстрее получать доступ к контенту, что повышает шанс вовремя удовлетворить ту или иную потребность. 62% пользователей поколения миллениалов (или просто – поколение Y) предпочитают совершать покупки и просматривать товар именно через приложение из-за высокой степени персонализации предложений и скорости оформления сделки.

Прецизионность и доходность: приложения стимулируют развитие таких технологий, как геолокация (точность определения местоположения) и голосовой поиск. Приложения создают своего рода сводную таблицу потребностей, т. е. помимо изображения пользователя, здесь есть информация об увлечениях: что они делают и что им нравится. Все в одном месте! Эта «сводная таблица» содержит точные сведения, которые можно использовать для повышения персонализации со стороны разработчика или продавца товара/услуг. Фактически 72% медиа-ресурсов, передававшие такие точные данные для брендов, зафиксировали увеличение продаж более чем на 50%.

Надежный доступ: пользователи устанавливают мобильные приложения на свои устройства в надежде получить актуальный и нужный контент. Доказано, чтобы получить более релевантный (максимально подходящий под запрос) контент, пользователи готовы раскрывать свои персональные данные.

Ориентированность на пользователя

Как уже и говорил выше, среднее количество установленных мобильных приложений в одном смартфоне - 35, но только 5 из них используются наиболее часто. Некоторые могут сказать, что это препятствие для развития индустрии. Тем не менее, доходы от приложений быстро растут и, как ожидается, будут расти в будущем.

Чтобы не отставать от быстро развивающегося цифрового (digital) рынка, мобильные разработчики должны убедиться в том, что еще на этапе создания приложения они больше ориентируются на потребительские требования и принимают во внимание существующие решения, в надежде доработать их. Пользователи теперь ожидают большей персонализации и адаптации под их местоположение.

Приложения лучше всего подходят для реализации этих возможностей благодаря грамотной интеграции технологий и услуг передачи данных:

Сервисы, основанные на местоположении – это быстро растущая категория, которая позволяет более эффективно настраивать таргетированную рекламу. Определяя наши направления, увлечения и основные места пребывания, маркетологи умело подбирают для нас подходящие коммерческие предложения. Технология мобильных платежей также стремительно растет, что позволяет быстро и эффективно совершать различные транзакции «в пути».

Как пользователи помогают созданию приложения?

Пользовательская проницательность – один из самых мощных инструментов в руках маркетологов и разработчиков. Огромное количество накопленной информации от пользователей (местоположение, интересы, привычки и т. д.) помогают быстрее находить приложениям с ними общий язык. Так или иначе, в наше время пользователи своими потребностями сами формируют рынок мобильных приложений.

Как приложения смогут влиять на поведение покупателей?

Поколение, которое никогда не жило в мире без мобильных устройств, требует более интерактивных приложений и рекламы. Основными ожиданиями от разработчиков являются релевантность и персонализация. Недавние исследования, проведенные Verve и Censuswide, показали, что пользователи в два раза чаще реагируют на мобильные

объявления, выданные на основе их местоположения по сравнению с общими объявлениями.

В итоге цифры...

Пример прогнозной статистики: к 2022 году оборот мировой мобильной экосистемы достигнет $4,6 трлн и составит 5% глобального ВВП. К 2025-му услугами индустрии будет пользоваться 5,9 млрд уникальных мобильных абонентов, или 71% ожидаемого населения Земли. Из них 5 млрд станут потреблять дата-трафик (сравните с 3,3 млрд в 2017 году)».

6.3. Рекомендации абонентам

Тема подключения контентных услуг нечасто поднимается средствами массовой информации.

Следующие статьи содержат рекомендации для абонентов. Внимание – актуальность информации о применяемых операторами процедурах не гарантируется!

- **Золотые номера России**
  https://kaluga.topnomer.ru/blog/kontentnyj-licevoj-schet.html

«Контентный лицевой счет

Сервисы мобильных операторов уже давно вышли за рамки обычных услуг связи. Однако, при использовании некоторых, у пользователей могут возникать неудобства. И основное, что вызывает раздражение у пользователей, развлекательные сервисы, которые в основном предоставляются не самими операторами связи, а их партнерами.

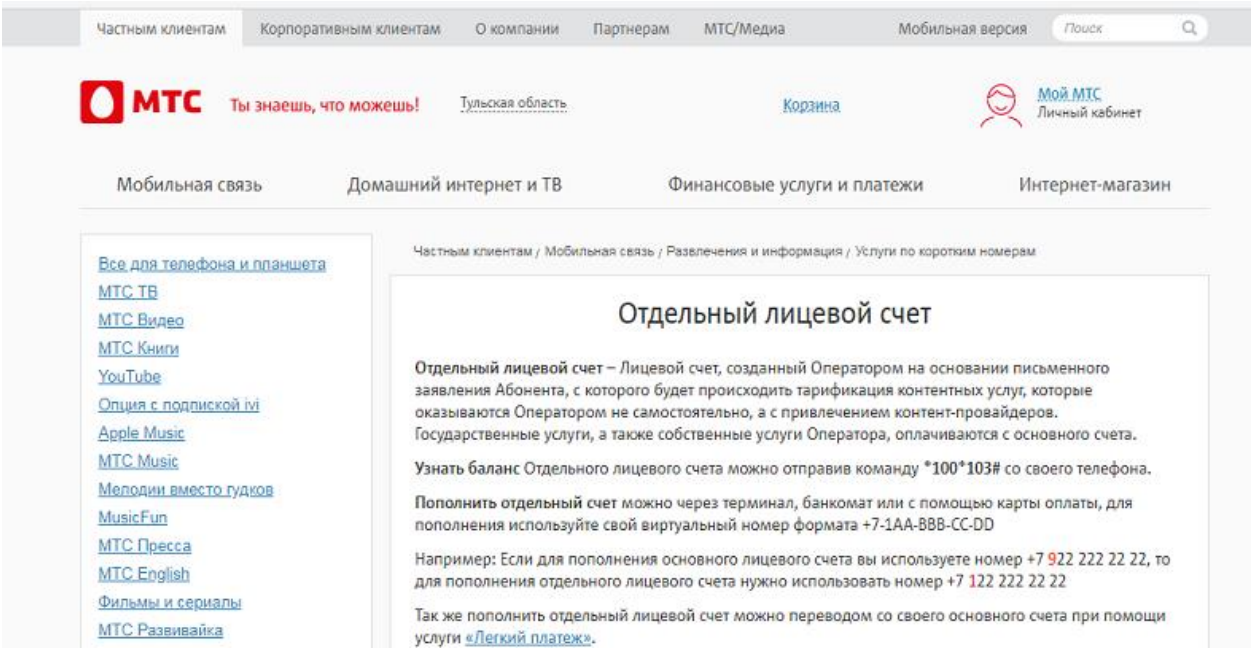
Подключение контентных услуг и подписок иногда может приводить не только к непредвиденным затратам для клиента любого сотового оператора, но и полному обнулению счета. Однако, клиент любого оператора может подключить отдельный контентный счет по своему номеру, чтобы избежать таких неприятных моментов, и сегодня расскажем про такую услугу на МТС, Билайн, МегаФон, и Теле2.

Для чего нужен отдельный счет

Есть различные услуги у сотовых операторов, позволяющие отключить заказ сервисов от контент-провайдеров на номерах Билайн, МТС, МегаФон, и Теле2. Однако, это не позволит полностью ограничить себя от непредвиденных списаний.

Это связано с тем, что не все контентные сервисы предоставляются самими операторами, и запрет на использование таких услуг и подписок, с помощью установки запрета, обычно подразумевает ограничение только на услуги от сторонних компаний. А вот если развлекательный сервис предоставляется через самого оператора, то бороться с ним гораздо сложнее.

В этом случае именно отдельный контентный лицевой счет позволит полностью ограничить себя от ото, что с баланса номера Теле2, МегаФон, Билайн, или МТС, такие списания будут продолжаться



Также есть и преимущества использования такого дополнительного баланса для тех, кто использует отдельные контентные услуги, но хочет ограничить себя от остальных. Так, к примеру, абонент Билайн использует развлекательные контент-услуги с заказом по номеру 5591, но в списке подключенных обнаруживает, что также есть платные сервисы по номеру 7944 или 6513, и хочет их отключить.

Именно отдельный лицевой счет позволит продолжать использовать и оплачивать нужные, но не использовать подключенные случайно. Имея отдельный баланс, пользователь сможет вносить на него деньги, только если нужно оплатить полезный ему контент.

Те, кто сталкивался со случайными списания за развлекательные сервисы, знают, что вернуть свои деньги практически нереально. Так, если абонент МегаФона случайно подключил доступ к контентному сервису, то чтобы вернуть деньги потребуется обращаться в ту компанию, которая предоставляет платный контент.

Как подключить отдельный баланс

Услуга предоставляется всеми сотовыми операторами, но найти информацию о ней крайне сложно на официальных сайтах. Нет возможности и подключить ее также быстро и легко, как оформить случайно подписку на платный развлекательный сервис.

Отдельный баланс предоставляется всеми операторами бесплатно, и можно не переживать, что потребуется вносить дополнительные платежи за его использование.

В зависимости от сотового оператора, услуга может называться по-разному, но ее смысла от этого не меняется. Так, на МТС и Билайн – это “Отдельный лицевой счет”, на Теле2 “Контентный лицевой счет”, а на МегаФоне просто “Контентный счет”. Для его использования необходимо обратиться к оператору лично в офис, и подать письменное заявление.

После подключения отдельного баланса для контента, абоненту становится доступен дополнительный виртуальный номер, используемый для оплаты развлекательных и информационных услуг.

Пополнять при необходимости дополнительный счет можно переводом с основного. Для этого у операторов доступны специальные команды.

Обратите внимание, что также есть возможность и обратного перевода денег с контентного на основной баланс. Однако после такого перевода использовать средства можно только на оплату услуги связи, как и при пополнении баланса с других обычных сотовых номеров.

Выводы

Использование отдельного счета для контентных услуг позволяет пользователю полностью ограничить себя от списания средств за развлекательные и информационные услуги. Для этого достаточно не вносить на него деньги. Так как запрет контента, доступный у любого оператора действует не на все платные сервисы, то используя отдельный баланс можно избежать случайных списаний.

Также сервис идеально подходит тем, кто использует некоторые контентные сервисы, и не хочет полностью блокировать доступ к ним. В этом случае можно пополнять отдельный баланс при необходимости оплаты нужных услуг, и избежать списаний при активации других».

- **Моё! Online – Как обезопасить себя от нежелательных платных подписок на телефоне?**
  https://moe-online.ru/news/pomozhem-razobratsya/358473

«Что делать, если с вашего телефона списывают деньги за услуги, о которых вы даже не знаете?

В последнее время активизировались жалобы воронежцев на то, что со счетов мобильных телефонов стали списываться деньги «неизвестно за что». Как правило, речь идёт об SMSках из разряда: «Вы активировали платную подписку. Абонентская плата 30 руб. в день. Сервис предоставлен компанией такой-то». «А я ведь даже ни на что не нажимал», – уверяют большинство попавших в такую ситуацию. Кто навязывает нам платные подписки и как с этим бороться?

Что такое платный контент?

Это может быть платная игра, приложение, подписка на новости, прогноз погоды или курсы валют. Причём услугу чаще всего предоставляет не оператор мобильной связи («Билайн», «Мегафон», МТС или «Теле2») а некий провайдер, у которого с оператором заключён договор на предоставление контент-услуг и которому выделен отдельный короткий номер (как правило, SMSки о платных подписках приходят с четырёхзначных номеров).

Причём юридически придраться к операторам сложно. На своих официальных сайтах они заранее предупреждают абонентов, что контент-услуги предоставляются сторонними провайдерами, что ответственности за них оператор практически не несёт (мол, вы сами на них подписываетесь). А в случае противоправных действий контент-провайдеров абонент вправе пожаловаться на них оператору. И если эта жалоба окажется обоснованной, оператор может заблокировать провайдера, лишив его короткого номера.

Как можно «подцепить» на телефон платную подписку?

Способов подловить абонента у контент-провайдеров много. Автоматическим согласием на оказание платной услуги может быть отправка SMS или звонок на короткий номер, оставление вашего номера телефона на торрент-ресурсах (якобы для регистрации).

Люди, не пользующиеся интернетом, часто попадаются, случайно нажав «ОК» на высветившемся на экране навязчивом баннере из разряда «Хочешь самый точный прогноз погоды?»

Но чаще платные подписки ловят, переходя по ссылкам в интернете (речь идёт о мобильном интернете 3G или 4G). Достаточно кликнуть интересную новость, нажать кнопку «скачать» или «lay» для воспроизведения видео, и всё – вы подписались на платную рассылку. По закону провайдер обязан вас предупредить о платной подписке. Но он делает это едва различимым мелким шрифтом, серым по чёрному внизу страницы, докуда не все даже долистывают.

Как проверить, есть ли у вас платные подписки, и отключить их?

Проще всего проверить наличие у вас платных подписок или услуг (и отключить их) можно в личном кабинете на сайте вашего оператора. Чтобы зайти в личный кабинет, как правило, нужно указать на сайте свой телефон, после чего вы получите SMS с кодом доступа или паролем.

Если у вас нет под рукой интернета, помните: когда вы (даже случайно) подписываетесь на платный контент, вам должно прийти соответствующее SMS с четырёхзначного номера. С приходом этого сообщения с вашего счёта уже списывается плата за первый день услуги (как правило, 20 – 30 руб.). Чтобы отключить услугу, отправьте в ответном сообщении на этот короткий номер слово СТОП или STOP. Отправка сообщения бесплатна.

Как обезопасить себя от нежелательных платных подписок?

Самый простой и верный способ – создать отдельный счёт для платного контента. С вашего основного счёта будут оплачиваться звонки, SMS и интернет. А если вы вдруг случайно подпишетесь на платную услугу, контент-провайдер сможет списывать деньги только со второго, контентного счёта. Если на этом счету будет 0 рублей, то, соответственно, и списываться ничего не будет. Если же вы сами захотите подписаться на какой-либо платный контент (прогноз погоды, новости и т. п.), то вам нужно будет пополнить свой контентный счёт на требуемую сумму. Контентный счёт – это 11-значный номер, который отличается от вашего мобильного номера на одну цифру. К примеру, 6 вместо 9 в префиксе, то есть вместо 8-903 в нём будет 8-603. Пополняется он так же, как счёт обычного телефона.

Конечно, контент-счёт – это не панацея. Некоторые операторы (например, «Мегафон») на контентном счёте предоставляют обязательный кредитный лимит, что может загнать вас в небольшой минус (подробнее об этом читайте ниже). Кроме того, существуют хитрости, когда операторы могут списывать деньги за платные услуги (если это собственный контент операторов) с основного счёта, даже при наличии контентного. Но такие подписки вы уже вряд ли подцепите случайно, перейдя по ссылке на незнакомом сайте.

Завести контентный счёт бесплатно можно в салоне сотовой связи конкретного оператора, прихватив с собой паспорт и написав соответствующее заявление по образцу. Есть и другие способы обезопасить себя от платных подписок. Рассмотрим все эти способы для каждого оператора подробнее.

«Билайн»

Для подключения контентного счёта наберите команду *110*5062# и нажмите вызов (запрос бесплатный). Проверка баланса отдельного счета – *622#. Команда перевода денег с основного баланса на дополнительный – *220*{сумма}# (к примеру, для перевода 100 рублей надо набрать *220*100#). Команда перевода денег с дополнительного баланса на основной – *222*{сумма}#. Команда для отключения дополнительного баланса – *110*5060#.

«Мегафон»

Открыть контентный счёт в «Мегафоне» можно только в салонах связи (с паспортом). «Мегафон» – единственный из операторов большой четвёрки, кто предоставляет обязательный и неотключаемый кредитный лимит на контентном счёте. То есть позволяет загонять счёт в минус – правда, максимум на 150 рублей. После этот счёт блокируется, но 150 рублей вы уже должны.

Однако безо всякого контентного счёта в «Мегафоне» можно запретить мобильные подписки, отправив SMS с текстом УСТЗАПРЕТ1 на номер 5051 (услуга бесплатная). Правда, запрет установится сроком на 3 месяца. Но по истечении этого срока оператор заблаговременно напомнит вам в SMS, что услугу можно продлить.

МТС

Открыть контентный счёт в МТС можно только в салонах связи (с паспортом). Однако у оператора МТС есть бесплатная услуга «Запрет контента», которая не даёт отправлять и принимать платные SMS и звонки с коротких номеров и защищает от случайных платных подписок. Подключается услуга по номеру 0890. Проверить, есть ли у вас платные подписки, и отключить их можно, набрав команду *111*919# (и вызов).

«Теле2»

Для подключения контентного счёта наберите команду *160# и нажмите вызов (услуга бесплатная). *160*1# – справка о балансе контентного лицевого счёта. *160*{сумма}# – перевод средств с основного счёта абонента на контентный. *160*{сумма}*0# – возврат средств с контентного счёта на основной. *152*0# – команда отключения платного контента и платных подписок, если они у вас уже имеются».

- **Комсомольская правда – Новый вирус подписывает смартфоны на платные сервисы**
  https://www.kp.ru/daily/26701/3725922/

«Вредоносная программа работает по схеме троянца

Эксперты «Лаборатории Касперского» обнаружили новый вирус, который незаметно для владельцев подписывает смартфоны на платные сервисы. Троянец под названием Xafekopy делает это, кликая по ссылкам, или с помощью отправки SMS.

Примечательно, что вредоносная программа даже научилась обходить капчу – тест для распознавания человека или автоматической системы при вводе каких-либо данных.

Как отмечают программисты, новый вирус напоминает троянц Ztorg. Более того, есть предположение, что создатели одного вируса могли купить или украсть часть файлов у создателей другого.

Сообщается, что в первую очередь новый вирус был направлен на пользователей из России и Индии. 61% и 25% всех атакованных проживают именно в этих странах соответственно. Всего в настоящее время зафиксировано уже 3816 случаев заражения гаджетов.

К слову, в России троянец получил отдельную модификацию. Вирус научился заходить на сайты четырех крупнейших операторов сотовой связи в стране и получать подтверждение подписки на платные сервисы.

Эксперты предупреждают, что вирус распространяется под видом полезных программ через рекламные сети. Интересно, что программа даже содержит полезный функционал. Это сделано для того, чтобы магазинам приложений и модераторам рекламных сетей было труднее идентифицировать программу как вредоносную.

«Мы наблюдаем развитие сотрудничества киберпреступников между собой, и государственные границы их не останавливают. Во-первых, два различных троянца используют похожие вспомогательные файлы: скорее всего, это стало следствием совместной работы двух группировок. Во-вторых, кибермошенники из одной страны воруют деньги у пользователей из других стран, вероятно, пользуясь помощью местных злоумышленников», – заявил Роман Унучек, антивирусный эксперт «Лаборатории Касперского».

Добавим, что помимо России и Индии вирус атаковал пользователей из Мексики, ЮАР, Турции и других стран».

7. Кейс «Недействительный полис ОСАГО»

При работе над кейсом обратите внимание на положения Федерального закона "Об обязательном страховании гражданской ответственности владельцев транспортных средств", касающиеся порядка оформления страховых полисов, а также обязывающие всех страховщиков продавать электронные полисы каждому обратившемуся за таким полисом страхователю (статья 15 Закона).

7.1. О схемах и случаях мошенничества с электронным полисом ОСАГО: обзоры и рекомендации

- **Российская газета – ЦБ предупредил о новой схеме мошенничества с полисами е-ОСАГО**
  https://rg.ru/2018/07/26/cb-predupredil-o-novoj-sheme-moshennichestva-s-polisami-e-osago.html

«Банк России рассказал о новом способе обмана автовладельцев, оформляющих электронные полисы ОСАГО через посредников.

Схема проста: посредник занижает стоимость страховки, вводя на сайте страховой компании недостоверные данные о транспортном средстве. К примеру, указывает, что страхуемый автомобиль является мотоциклом. После получения от страховщика полиса в документ вносятся изменения с помощью обычного графического редактора. Автовладелец платит за полис уже реальную сумму страховки.

Так как страховщик не получил страховую премию, соответствующую установленным страховым тарифам, такой договор ОСАГО может быть признан недействительным, предупреждает ЦБ в своем разъяснительном письме. Это значит, что в случае ДТП владельцу такого полиса придется самостоятельно нести ответственность.

Подобная практика обмана автолюбителей посредниками в последнее время получила широкое распространение, отмечают в Банке России. Регулятор предупреждает, что страховая компания вправе отказать в заключении договора ОСАГО в электронном виде, если электронное заявление подано лицом, которое не является собственником автомобиля или не допущено к управлению автомобилем».

- **РБК – Базовая несостыковка: как мошенничают с электронными полисами ОСАГО**
  https://www.rbc.ru/finances/09/10/2017/59d78d609a7947c35ddd9712

«До 10% проданных в этом году электронных полисов ОСАГО могут содержать недостоверные данные. Их предоставляют страховым компаниям без ведома автовладельцев посредники, добивающиеся для себя минимальной цены полиса.

На российском страховом рынке получила широкое распространение новая схема мошенничества с электронными полисами ОСАГО (е-ОСАГО). Об этом РБК рассказали в компании «Ингосстрах» и подтвердили еще в пяти крупных страховых компаниях.

Речь идет о том, что компании-посредники, предлагающие водителям услугу оформления е-ОСАГО, намеренно подают страховщикам недостоверные сведения, добиваясь снижения стоимости полиса. Эксперты оценивают долю таких полисов примерно в 5–10% (250–500 тыс. штук) в структуре электронных продаж ОСАГО.

В Центробанке заявили, что регулятор «в курсе появления подобных схем на страховом рынке». «В настоящее время совместно с представителями страхового сообщества вырабатываем комплекс технологических и нормативных мер, направленных на предотвращение подобных проявлений», – говорится в заявлении ЦБ, поступившем в РБК. Там также отметили, что нужно оповещать автовладельцев «о негативных последствиях, которые могут возникнуть после обращения к такого рода посредникам».

По результатам опроса РБК, который охватил топ-10 российских страховых компаний по объему страховых премий в сегменте ОСАГО (данные ЦБ за первое полугодие 2017 года), наличие проблемы с недобросовестным оформлением полисов е-ОСАГО подтвердили в «РЕСО-Гарантии», «АльфаСтраховании», «Росгосстрахе», ВСК и МАКСе.

В «Ренессанс Страховании», «Югории», «Согласии» и СОГАЗе не ответили на запросы.

В Российском союзе автостраховщиков (РСА) также подтвердили, что с популяризацией е-ОСАГО страховые компании начали чаще сталкиваться со случаями предоставления недостоверных данных при оформлении полисов.

Как действуют мошенники

«Мошенники начали массово приобретать электронные полисы ОСАГО (е-ОСАГО), оформляя их на наиболее дешевые по стоимости полиса модели автомобилей с низкой мощностью и в регионе, где самые низкие коэффициенты, но указывая регистрационный номер и VIN (идентификационный номер транспортного средства) реального покупателя. В результате за полис мошенники платят, условно говоря, 1000 руб. Затем они изменяют с помощью фоторедактора данные водителя в полисе в соответствии уже с его регионом и моделью авто и продают его покупателю, условно, за 15 тыс. руб. в зависимости от региона, а разницу кладут себе в карман», – рассказал генеральный директор «Ингосстраха» Михаил Волков.

«В отличие от бумажной формы при подаче электронного заявления у представителя страховщика отсутствует возможность оперативной проверки информации», – пояснили РБК в пресс-службе РСА. Мошенники меняют разные данные – о стаже водителя, возрасте автомобиля и т.п., чтобы добиться нужного результата, рассказал РБК официальный представитель «АльфаСтрахования» Юрий Нехайчук. «Либо меняют регион преимущественного использования на регион с минимальными коэффициентами, таким способом добиваясь снижения цены», – добавил он.

На данный момент база данных РСА, которая проверяет данные водителя, когда оформляется е-ОСАГО, не способна автоматически при оформлении электронного полиса на сайте проверять данные марки автомобиля и его регион из базы данных ГИБДД, которая содержит такую информацию, дополняет заместитель гендиректора «РЕСО-Гарантии» Игорь Иванов.

Например, в таких регионах, как Крым и Чечня, самые низкие территориальные коэффициенты – 0,6, тогда как в Москве и Санкт-Петербурге они в три с лишним раза выше – 2. И если рассчитать минимальную стоимость полиса ОСАГО на сайте РСА для машины самой низкой мощности (50 л.с.), для водителя с наименьшим периодом использования ТС (три месяца), но с самым большим коэффициентом стажа (от трех лет) и возраста (от 22 лет) в Крыму или Чечне, то страховая премия будет от 617,76 до 741,24 руб. В то же время

максимальная стоимость полиса для Москвы и Санкт-Петербурга по максимальным параметрам для легкового автомобиля (самая высокая мощность – 150 л.с., период пользования ТС – от десяти месяцев и больше, с самым низким стажем – до трех лет и возрастом водителя – до 22 лет) страховая премия будет от 19 768,32 до 23 719,68 руб.

При этом с таким полисом можно долго и благополучно ездить. Сотрудники ГИБДД проверяют полис формально и обращают внимание больше на его наличие, чем на действительность, поясняет юрист правового департамента HAEDS Consulting Анастасия Худякова.

Даже если сотрудник ГИБДД при проверке полиса ОСАГО пользуется базой РСА, в которой находятся данные всех полисов, он может не заметить несовпадений, говорит Игорь Иванов. «В базе высвечиваются верные данные о госномере автомобиля и номере VIN, а на несовпадение данных по региону или марке машины обычно не обращают внимания», – поясняет он.

Проблемы у владельца автомобиля возникают в случае обращении в страховую компанию после ДТП. Там и выявляют подделку, уточняет Худякова. В результате страховая отказывает в выплате, поскольку в базе РСА, несмотря на совпадение госномеров и VIN, другие данные расходятся.

Как оформляется полис е-ОСАГО

С 1 июля 2017 года вступили в силу поправки в закон об обязательном страховании автогражданской ответственности, которые позволяют оформлять полисы ОСАГО в режиме онлайн на сайтах страховых компаний. Согласно порядку заключения договора ОСАГО в виде электронного документа, для этого необходимо сделать следующее:

– зайти в личный кабинет на сайте страховщика (зарегистрироваться на сайте страховщика или зайти через портал государственных услуг Российской Федерации);
– в личном кабинете заполнить заявление о заключении договора.

После заполнения заявления осуществляется проверка указанных в нем данных через автоматизированную информационную систему РСА (АИС РСА). После подтверждения соответствия представленных сведений сведениям, содержащимся в АИС РСА, либо проверки электронных копий документов страховщик отображает на сайте расчет страховой премии. После оплаты страховой премии электронный полис направляется на адрес электронной почты страхователя и размещается в его личном кабинете. Полученный электронный полис ОСАГО необходимо распечатать и иметь при себе при управлении транспортным средством. Электронный полис ОСАГО имеет такую же юридическую силу, как и страховой полис, оформленный на бланке строгой отчетности в офисе страховщика.

Почему мошенничество стало популярным

С начала этого года продажи полисов е-ОСАГО растут лавинообразно, после введения требования об обязательности этой формы продаж для страховых компаний, рассказали РБК в пресс-службе РСА. На текущий момент доля полисов с недостоверными данными оценивается примерно в 5–10% в структуре электронных продаж ОСАГО (с начала года продано 4,7 млн полисов е-ОСАГО).

Электронное ОСАГО вводилось для защиты от «уличных брокеров» и для удобства клиентов – чтобы автовладелец мог оформить полис, не выходя из дома. Реальность же такова, что некоторые из них плохо владеют компьютером или не хотят тратить время на заполнение полиса, говорит Игорь Иванов. «Для е-ОСАГО надо сканировать различные документы, и в среднем его заполнение может занять около часа, поэтому человек ищет альтернативный способ и обращается к «помощникам» на стороннем сайте, которые могут оказаться мошенниками», – поясняет Иванов.

«Мошенниками могут выступать в основном посредники с сайтов, которые предлагают в интернете оформить за водителя полис е-ОСАГО. И тут нельзя определить наверняка, реальный ли это посредник или выдающий себя за такого, – говорит Игорь Иванов. – Потому что е-ОСАГО само по себе не подразумевает использование кого-то еще для его оформления. На данный момент работа таких сайтов никак не урегулирована».

Проблема с частично не совпадающими данными в проданных полисах и в базе данных РСА стала на «промышленные рельсы» из-за того, что мошенники могут на одного человека оформить сразу несколько полисов с разными госномерами и VIN-номерами и по самому низкому тарифу, говорит Михаил Волков. «Ситуация тяжелая, потому что вся эта система только внедрена на рынке. Предусмотреть все возможные проблемы, которые очень быстро находят мошенники, невозможно», – поясняет он.

К обращению к посредникам могут невольно подталкивать и сами страховые компании, многие из которых не хотят продавать электронные полисы ОСАГО в так называемых токсичных регионах, где наблюдается высокая убыточность по выплатам, о чем ранее писал РБК.

У клиента, который пытается по всем правилам оформить себе е-ОСАГО на машину из «токсичного» региона, могут возникать проблемы с загрузкой данных, постоянным обновлением страницы, где требуется снова и снова вводить данные, и в итоге он прибегает к помощи на стороне, говорит генеральный директор Mains Group Сергей Худяков. Мошенники, в свою очередь, указывают данные, соответствующие целевому сегменту страховой компании в регионах, где страховщику выгодно их продавать, при этом добиваясь выгодных коэффициентов для покупки самого дешевого полиса, добавляет он. «В результате они беспрепятственно покупают полис на сайте страховой компании для ничего не подозревающего клиента, а потом в компьютерных программах-редакторах меняют данные марки авто и региона и продают полис по цене для «токсичного» региона», – поясняет Худяков.

Сами автовладельцы также могут быть экономически заинтересованы в том, чтобы приобрести дешевый страховой полис, намеренно вводя неверные данные, например по территории преимущественного использования ТС, чтобы снизить размер премии, особенно в регионах, где высокие тарифы, говорит партнер FMG Group Михаил Фаткин. «Между гарантированным законом страхованием ответственности и дешевым полисом с некорректными данными водители целенаправленно выбирают дешевизну полиса и получают видимость того, что застрахованы, – для ГИБДД», – разъясняет он.

Как уберечься от мошенничества

В страховых компаниях говорят, что покупка полиса ОСАГО у посредника чревата обманом.

В случае разночтения сведений, содержащихся в полисе страховщика, и полисе, скорректированном с помощью фоторедактора недобросовестными посредниками, страхователь не может рассчитывать на получение страхового возмещения – основанием для отказа является соответствующее положение п. 2 ст. 6 федерального закона об ОСАГО, отметили в пресс-службе ВСК. Там также сообщили, что количество случаев отказа на этом основании «сегодня исчисляется сотнями».

В «Ингосстрахе» выявлено около 40 случаев отказа страхователю в выплате из-за несовпадения данных, сообщили в пресс-службе компании. В «Рогосстрахе» говорят о десятках жалоб в неделю. «Первые случаи обмана автовладельцев были зафиксированы нами еще весной. А уже к лету это явление приобрело массовый характер и продолжает разрастаться. Общий объем мошенничества сложно оценить, но мы уже получаем десятки жалоб в неделю – и это только от тех автовладельцев, которые уже столкнулись с последствиями владения фиктивными полисами», – заявил РБК вице-президент, руководитель департамента развития прямых продаж «Росгосстраха» Ренат Конурбаев.

Если факт подделки полиса обнаружит инспектор ГИБДД, это чревато возбуждением дела об административном нарушении по ст. 12.37 КоАП «Несоблюдение требований об обязательном страховании гражданской ответственности владельцев транспортных средств» с минимальным штрафом 800 руб., говорит Анастасия Худякова. При обращении за выплатой в страховую компанию в случае, если выяснится, что полис поддельный, высока вероятность привлечения держателя полиса к уголовной ответственности по ст. 327 УК (подделка документов) и ст. 159.5 УК (мошенничество в сфере страхования), поясняет она.

В случае виновности в ДТП владелец поддельного полиса все равно будет вынужден компенсировать ущерб пострадавшему. Ведь он не сможет получить страховую выплату – компания не признает страховой полис из-за некорректных данных, говорит Фаткин. В данном случае пострадавший имеет право обратиться с иском в суд и через него взыскать с виновника ущерб, поясняет он. Такая практика уже существует – к ней прибегают, например, когда страхового покрытия, гарантированного полисом, не хватает для полного покрытия ущерба. В этом случае пострадавший также направляется в суд и успешно взыскивает остаток, поясняет юрист. «В случае, когда обнаружится, что страховая не выплатит вообще ничего из-за поддельного полиса, невиновный пострадавший имеет все шансы взыскать через суд у виновника ДТП с поддельным полисом средства за причиненный ущерб», – заключает юрист.

Чтобы избежать всего этого, говорят эксперты, необходимо проверить приобретенный полис по базе РСА на предмет его подлинности и соответствия внесенных в него данных действительности.

Обычно после того, как страхователь оформил полис е-ОСАГО на сайте страховой компании, данные о нем добавляются в базу РСА в течение 30 минут, говорит Юрий Нехайчук. «Проверить полностью все данные в базе с теми, что указаны в его полисе, клиент может самостоятельно на сайте РСА», – поясняет он.

Если после проверки самостоятельно введенных данных е-ОСАГО водитель обнаружил, что допустил ошибку при вводе, например в фамилии, или неправильно указал мощность машины, то он должен прийти в офис компании и написать заявление на

изменение данных, после чего ему либо просто исправят ошибку в полисе, либо проведут перерасчет, добавляет Юрий Нехайчук.

Когда проверка указывает на признаки возможного мошенничества со стороны посредников или страховщика, необходимо незамедлительно обратиться в полицию с заявлением, указав, при каких обстоятельствах, где, когда и у кого был приобретен полис. Процедура это стандартная, дальше поиском мошенников будут заниматься правоохранительные органы, говорит Худякова. «При этом, приобретая электронные полисы на сторонних сайтах, можно предположить, что найти таких мошенников будет затруднительно, так как наши правоохранительные органы до сих пор не любят заниматься расследованием таких нарушений», – добавляет юрист. Фактически неизвестно, насколько активно правоохранительные органы будут расследовать данные нарушения и будут ли вообще, и поэтому сроки возмещения ущерба могут затянуться, заключает Худякова.

Если водителя обманул посредник, то в его действиях есть признаки преступления по статье «Мошенничество в сфере страхования», но для доказательства того, что водителю действительно продали поддельный полис с исправленными данными, пострадавшему необходимо будет предоставить все платежные документы, отмечает Михаил Фаткин. «Иначе доказать, что он действительно приобрел полис у конкретного лица, будет практически невозможно», – заключает он.

Где системный выход из проблемы

Ситуация может быть исправлена путем создания единой базы ГИБДД, имеющей объединенный интерфейс с базой РСА, считает заместитель генерального директора СК «МАКС» Виктор Алексеев. «В этом случае при оформлении полиса е-ОСАГО автоматически должен уходить запрос в базу ГИБДД за подтверждением введенных данных об автомобиле. Если имеются несовпадения, полис не оформляется», – пояснил он.

РСА направил в Банк России предложения по усовершенствованию указания «О требованиях к использованию электронных документов и порядке обмена информацией в электронной форме при осуществлении обязательного страхования гражданской ответственности владельцев транспортных средств», рассказали в пресс-службе организации (имеются в распоряжении РБК). В ЦБ не ответили на запрос РБК относительно подготовленных поправок.

Документом, в частности, предлагается дать возможность страховой компании при оформлении е-ОСАГО в случае возникновения подозрений, что клиент намеренно мог занизить коэффициенты для покупки полиса, проводить дополнительную проверку данных с использованием источников, содержащих информацию, имеющую значение для определения размера страховой премии, говорится в документе. «К таким источникам, в частности, относятся интерактивные сервисы федеральных органов исполнительной власти и органов власти субъектов Федерации, общедоступные источники персональных данных, официальные данные заводов – изготовителей транспортных средств, при этом такая проверка осуществляется в срок не более 20 минут с момента получения ответа из АИС РСА», – поясняется в документе.

Также среди мер, которые могли бы пресечь мошенничество в е-ОСАГО, у страховой может появиться возможность расторгать в одностороннем порядке договоры, составленные с явными нарушениями. «Предоставление недостоверных данных при

заключении ОСАГО должно быть основанием для одностороннего расторжения договора», – пояснили РБК в пресс-службе. Сейчас в момент продажи бумажного полиса страховщик имеет право отказать в заключении договора, при электронном – не может, только через суд, добавили там. «Наличие возможности расторгнуть такой договор в одностороннем порядке также решило бы проблему», – заключили в пресс-службе».

- **Автомотопроф – Новая схема обмана и мошенничества с электронными полисами ОСАГО**
  http://avtomotoprof.ru/obman-i-moshennichestvo-s-elektronnyimi-polisami-osago/

Материал по ссылке содержит описание схемы мошенничества с электронными полисами ОСАГО, а также мнение авторов материала о причинах распространения такой схемы и рекомендации автовладельцам.

- **Sravni.ru – 4 вида мошенничества при продаже ОСАГО, и как их избежать**
  https://www.sravni.ru/text/2017/12/12/4-vida-moshennichestva-pri-prodazhe-osago-i-kak-ikh-izbezhat/

«Только за первое полугодие 2017 года страховщики отправили в полицию почти 2 тысячи заявлений о подделке полисов ОСАГО. Для тех, кто по каким-то причинам покупает страховки не на Сравни.ру, рассказываем, как обманывают при продаже ОСАГО, и как этого избежать.

1. Поддельный полис

Как это работает

Человеку поступает звонок, и ему сообщают, что полис можно приобрести по выгодной цене. Как правило, она ниже установленной законом, то есть ниже страховых тарифов. Люди верят и думают, что действительно по какой-то причине с рук смогут купить полис дешевле, и затем соглашаются. Курьер привозит им полис на бланке и забирает деньги. «Позже выясняется, что этот полис на самом деле к страховой компании не имеет никакого отношения, либо его бланк числится как испорченный или утерянный», – рассказывает адвокат Московской городской коллегии адвокатов Григорий Колесников. То есть если случится авария, страховая платить не будет.

Такие поддельные бланки также часто продаются в нестационарных пунктах, микроавтобусах, которые паркуются вблизи автосалонов, пунктов прохождения техобслуживания или авторынков.

«Как правило, действия мошенников построены таким образом, чтобы не дать возможности страхователю проверить подлинность полиса, – рассказывает юрист правового департамента Heads Consulting Игорь Валуев. – А в случае если он все-таки обращается к базе РСА, ссылаются на регулярные технические ошибки, которые якобы случаются уже не в первый раз, либо на то, что полис еще не внесен в базу, и на это нужно время».

Кроме штрафа за передвижение без действительного полиса ОСАГО (800 рублей), в случае аварии вам придется оплачивать ремонт за свой счет.

Как избежать

Тут всё просто. Действительный полис ОСАГО всегда найдется при проверке в РСА. Также можно позвонить в страховую компанию, продиктовать номер бланка, и сотрудник компании сообщит, в каком статусе находится этот бланк (утерян, похищен, выдан агенту, оформлен на другое лицо и т.д.).

2. Неверные данные об автомобиле

Как это работает

Этот вариант мошенничества возможен в случае с покупкой электронного полиса ОСАГО. Мошенники оформляют на сайтах страховщиков электронный полис на подставной автомобиль, указывая VIN и номер транспортного средства, полученный из баз ГИБДД, которые регулярно появляются на «чёрном рынке». Полис оформляется с минимальной премией, а далее мошенники предлагают его жертве, но уже с премией, соответствующей конкретному автомобилю.

«Данные в уже оформленном на подставное транспортное средство электронном полисе ретушируются на новые, – рассказывает Игорь Валуев. – Фактически полис является подлинным, он зарегистрирован в базе РСА, но получить возмещение по нему невозможно, поскольку по факту этот полис зарегистрирован на другой автомобиль».

Как избежать

Если вы покупаете полис у агента, то распознать такой способ мошенничества сложно. Но если вы самостоятельно покупаете полис онлайн, то проблем возникнуть не должно.

Если по каким-то причинам вы всё-таки хотите покупать полис у страхового брокера или агента, то Игорь Валуев из Heads Consulting советует обращаться в офисы крупных страховых компаний.

3. Неверный региональный коэффициент

Как это работает

Президент Ассоциации защиты страхователей Николай Тюрников рассказывает, что брокеры могут проделывать трюк со снижением регионального коэффициента. Этот коэффициент может значительно сократить конечную стоимость полиса. Так, самый низкий коэффициент – 0,6 – действует в таких регионах, как Крым, Калмыкия, Ингушетия и т.д. Самые высокие – в таких городах, как Челябинск (2,1), Мурманск (2,1), Москва (2), Казань (2), Санкт-Петербург (1,8) и др.

«Брокер может ввести неверные данные о регионе присутствия, например, москвичу оформить полис с коэффициентом Крыма», – рассказывает Николай Тюрников.

Это может произойти как в сговоре с автовладельцем, так и без ведома клиента. В первом случае страховщик и покупатель делят экономию пополам. Во втором – автовладелец платит полную стоимость и не знает, что полис выписан с преимущественным использованием в другом регионе. Брокер, в свою очередь, кладёт разницу в стоимости себе в карман.

Если в вашем полисе будут ложные данные, то страховая компания заставит заплатить по убытку человека, который предоставил заведомо ложные данные.

Как избежать

Перед покупкой полиса рассчитать его стоимость самостоятельно. Кстати, в разных страховых стоимость полиса для одного и того же водителя может отличаться на 20%.

Если вы этого не сделали, Григорий Колесников из Московской городской коллегии адвокатов в общении со страховыми агентами советует последовательно выяснять подробности, задавать вопросы, интересоваться. «Уже это может в значительной степени защитить вас от мошенников», – говорит он.

4. Фишинг

Как это работает

Мошенничество возможно и со стороны сомнительных онлайн-агрегаторов. В этом случае автовладелец находит в интернете сторонний сайт, который может оказаться фишинговым, имитировать продажи полисов. Сомнительный ресурс может также оказаться «клоном» сайта одного из страховщиков.

Кроме продажи несуществующих полисов поддельный сайт получает и данные банковской карточки человека. «Сначала списываются деньги за полис, а затем мошенники могут использовать полученные банковские данные для других операций», – предупреждает Николай Тюрников.

Как избежать

Самый простой путь обезопасить себя – покупать полис на официальном сайте страховой компании (их перечень есть на сайте ЦБ). А онлайн-сервисами можно пользоваться только теми, которым лично вы доверяете.

Также никто не отменял базовых правил осторожности, которых следует придерживаться в интернете в принципе:

- пользоваться картой, поддерживающей технологию 3D-Secure;
- завести отдельную карту для покупок в интернете и переводить на нее нужную сумму денег через интернет-банк или мобильный банк;
- регулярно проверять свой компьютер с помощью обновлённых антивирусных программ;
- не пересылать информацию о своей карте с помощью средств компьютерной связи;
- пин-код вашей карты для онлайн-платежей не нужен, сообщать его никому нельзя».

- **INGURU Страхование – Как не стать жертвой мошенников при покупке ОСАГО?**
  https://www.inguru.ru/kalkulyator_osago/stat_moshennichestvo_osago

«Навязывание дополнительных услуг и отказы в продаже полисов ОСАГО вынуждают страхователей прибегать к услугам сомнительных личностей. В результате многие автомобилисты по собственной неосмотрительности покупают фальшивые

страховки. Какие меры стоит предпринять, чтобы исключить возможность покупки подделки?

Отличительные признаки оригинального бланка

Полис ОСАГО – не просто важный документ, подтверждающий факт заключения страхового договора. Оригинальные бланки, используемые автостраховщиками, печатают на фабриках «Гознака». Изготовить такой документ в кустарных условиях практически невозможно, ведь бланк полиса ОСАГО обладает несколькими степенями защиты. Отличительными признаками настоящего бланка являются:

- разноцветные защитные волокна, светящиеся в ультрафиолете;
- рельефный индивидуальный номер;
- качественная типографская печать;
- водяные знаки с эмблемой РСА;
- вшитая металлическая линия.

Отсутствие любого из приведенных признаков свидетельствует о том, что перед автовладельцем поддельный полис. Кроме того, любой гражданин может проверить принадлежность бланка определенному страховщику. Для этого достаточно указать номер документа в специальной форме на сайте РСА . Система поможет определить, за какой страховой компанией закреплен конкретный бланк.

Отдельного внимания заслуживают похищенные оригинальные бланки. Злоумышленники могут заполучить настоящие полисы ОСАГО двумя способами: украсть в действующей страховой компании или приобрести у сотрудников обанкротившегося страховщика. В подобном случае довольно сложно самостоятельно выявить обман, ведь речь идет о настоящем бланке полиса. Следовательно, нужно обращать внимание не только на бланк, но и на поведение представителя страховой компании.

Как распознать мошенника?

Иногда проще распознать попытку обмана ориентируясь на поведение страхового агента. Даже если мошенник ранее работал в какой-либо страховой компании, он всё равно выдает себя странным поведением и неадекватной реакцией на простейшие просьбы клиента. Аферист ни при каких условия не согласится показать паспорт, ведь в таком случае не составит труда установить его личность, а значит мошенник не сможет избежать наказания. Кроме того, страхователю стоит насторожиться, если агент:

- отказывается предъявить агентский договор или доверенность, выданную страховщиком;
- не может сообщить корректное значение коэффициента бонус-малус;
- не пользуется базой данных РСА при оформлении полиса;
- не выдаёт квитанцию об оплате страховки;
- существенно занижает стоимость полиса;
- отказывается от безналичной оплаты;
- не требует диагностическую карту;
- заполняет полис от руки.

В случае малейших сомнений в честности страхового агента свяжитесь со страховой компанией, интересы которой представляет продавец.

Уточните в контактном центре, есть ли такой сотрудник в штате страховщика. Если не можете позвонить, как минимум зайдите на веб-сайт страховщика. На страничке любой отечественной страховой организации есть полный перечень посредников. Если агента нет в этом списке, с большой долей вероятности перед вами мошенник.

Последствия покупки подделки

Многие думают, что покупка поддельного полиса ОСАГО в худшем случае обернётся напрасной тратой денег. Однако последствия такого приобретения могут быть гораздо серьёзнее. Если владелец машины не сумел распознать обман на стадии оформления страховки, есть два пути выявления подделки.

1. Афера вскроется при внесении изменений в полис.
2. Афера вскроется при наступлении страхового события.

В первом случае придётся потратиться на покупку настоящего страхового полиса. А вот если автовладелец успел стать виновником аварии, последствия приобретения подделки будут куда печальнее. Придётся самостоятельно возмещать вред, причинённый чужому имуществу и здоровью. Кроме того, автовладелец может быть привлечён к уголовной ответственности, но только если будет доказано, что он сознательно приобрел поддельный полис.

При обнаружении подделки уже после завершения процедуры оформления стоит незамедлительно обратиться в полицию. Это позволит сотрудникам МВД принять оперативные меры по розыску афериста. Кроме того, заявление в полицию снимет со страхователя возможные подозрения в том, что он умышленно приобрёл поддельный либо недействительный полис ОСАГО.

Как купить настоящий полис?

Мошенники предпочитают проворачивать аферы в общественных местах: в метро, в подземных переходах, на авторынках и так далее. Нередко они готовы доставить полис в любое удобное для автовладельца место. Следовательно, желательно оформлять ОСАГО непосредственно в офисе страховой компании. Такой подход требует больше времени, зато позволяет избежать серьёзных неприятностей в будущем.

Если всё же предпочитаете пользоваться услугами страхового агента, стоит попросить посредника перенести заключение сделки в офис страховщика.

У настоящего агента не должно возникнуть с этим никаких сложностей. Офисы большинства отечественных компаний оборудованы рабочими местами для агентов. Таким образом, не придётся тратить время на ожидание в очереди к менеджеру, оформляющему «автогражданку».

Оформление полиса в офисе даёт ещё одно преимущество: можно внести платёж в кассу страховщика. Такой способ оплаты позволит избежать риска мошенничества со стороны действующего агента. Некоторые несознательные посредники не передают менеджерам второй экземпляр полиса и деньги, внесённые клиентом. Предсказать

последствия такого обмана почти невозможно, но он в любом случае не сулит ничего хорошего.

В качестве альтернативы можно оплатить страховую премию безналичным платежом. Это также позволит избежать риска присвоения денег агентом.

Электронная альтернатива

С 2017 года любой автовладелец может оформить договор ОСАГО в электронной форме. Такие страховки обязаны продавать все страховые компании, занимающиеся обязательным автострахованием. Полный перечень этих организаций приведён на сайте Российского Союза Автостраховщиков . Там же указаны адреса официальных сайтов страховщиков. Чтобы не столкнуться с мошенниками, подделывающими сайты страховых компаний, нужно ориентироваться на адреса из перечня на сайте РСА».

- **ЗеленоградСегодня – Полиция предупреждает о мошенничествах с полисами ОСАГО**
  https://zelenograd-news.ru/news/bezopasnost/politsiya_preduprezhdaet_o_moshennichestvakh_s_polisami_osago

«Как отличить поддельный полис ОСАГО от настоящего? Сколько водители готовы заплатить за фальшивку? Какая ответственность предусмотрена за такую покупку или за распространение фальшивых бланков? Можно ли вернуть потраченные на «левую» страховку деньги?

Полис ОСАГО является обязательным документом, дающим право эксплуатировать автомобиль на законных основаниях. Без страхования гражданской ответственности автовладельцев нельзя садиться за руль. При остановке сотрудниками ГИБДД такой водитель машины будет оштрафован в соответствии с положениями КоАП РФ. Некоторым владельцам авто страховка не по карману и они ищут более дешевые варианты приобретения документа – кто-то покупает липовые полисы ОСАГО по незнанию, кто-то делает это намеренно. Различают два их вида:

- Выполненный на настоящем бланке строгой отчетности;
- Полностью поддельный.

В первом случае для подлога используется настоящий бланк полиса, полученный незаконным путем. На нем может быть настоящий регистрационный номер, подписи и печати, но страховая компания, которой этот бланк принадлежал, его не оформляла и не продавала. Такие ситуации без участия недобросовестных сотрудников страховщика чаще всего невозможны. В случае, если компания недосчитывается полисов, то она сообщает об этом в РСА в форме отчетности, номер бланка заносится в базу как потерянный и получить по нему выплату страхового возмещения уже не получится.

Во втором случае полисы полностью поддельные. В зависимости от квалификации мошенников, их изготавливающих, документ может быть выполнен на хорошей бумаге с водяными знаками, с настоящими печатями и т.д., или на обычной бумаге – чаще такие «левые» документы просто распечатывают на цветном принтере. И отличить такую подделку от действительного полиса проще всего.

Признаки фальшивого бланка ОСАГО и как отличить поддельный полис? Усугубила ситуацию с мошенничеством новая норма законодательства, позволяющая водителям показывать инспектору ГИБДД на дороге простую распечатку полиса, купленного в электронном варианте. Если такой полис оформляется через недобросовестного посредника, а не напрямую на сайте страховой компании, вероятность наткнуться на подделку очень велика. Такие посредники обычно покупают бюджетный действующий ОСАГО, вносят исправления по данным покупателя, и получают за проданный документ в 3-4 раза больше, чем сами заплатили страховщику. Визуально определить, что этот документ является ненастоящим, не получится. Но есть несколько способов отличить фальшивку от настоящего бланка. К ним относятся следующие:

- Проверка внешнего вида полиса ОСАГО. Действующий бланк нового образца должен:
  - быть выполнен на бумаге высокого качества;
  - иметь печать страховой компании в верхнем углу слева;
  - иметь рельефный регистрационный номер;
  - иметь указание о том, что банк напечатан на типографии ГОЗНАК;
  - быть выполненным печатным способом, заполнение ручкой – явный признак фальшивки;
  - иметь на лицевой стороне микросетку голубовато-зеленого цвета, а также ворсинки красного и зеленого цвета, как на денежных знаках;
  - иметь водяные знаки по всему бланку с логотипом РСА;
  - иметь справа на обороте полоску металлического цвета.
- Проверка лицензии страховщика, от имени которого оформлен бланк полиса ОСАГО;
- Проверка самого полиса ОСАГО по его серии и номеру.

Проверку действительности полиса ОСАГО можно сделать на сайте РСА. Для этого в специальную форму нужно ввести серию и номер бланка, указанные на документе и нажать на кнопку «Поиск». Если автовладельцу продали поддельный полис ОСАГО, то после проверки появится запись о том, что полис с введенными реквизитами не найден. Лицензию страховщика можно проверить на сайте Центробанка. ЦБ регулярно обновляет реестры субъектов страхового дела и указывает в них всех действующих и лишенных лицензии страховщиков.

Сколько стоит «липовая» страховка

Купить поддельный полис ОСАГО можно как по очень низкой цене, так и по стоимости настоящего документа. Цены различаются из-за целей использования страховки. Водители, которые осознанно идут на подлог и покупают «липовый» бланк, делают это, чтобы просто демонстрировать документ сотрудникам ГИБДД. Цели получать страховое возмещение по такому полису у них нет.

Для водителей, которые и не подозревают о том, что покупают подделку, ОСАГО будет продаваться по цене настоящего – в среднем 5000-6000 рублей. Стоимость такого бланка будет зависеть от тех же показателей, по которым рассчитывается цена настоящей страховки – территории, возраста и стажа, мощности двигателя автомобиля, КБМ и т.д. Мошенники используют для расчета стоимости ту же методику, что и страховые компании.

Как и где можно купить недействительные полисы?

Мошенники предлагают купить бланк полиса ОСАГО через социальные сети, через сервисы объявлений, с помощью простой расклейки объявлений на улицах городов. Приобрести документ можно по стандартной для мошенников процедуре. Она чаще всего подразумевает звонок по оставленному номеру телефона, сообщение мошеннику данных, необходимых для заполнения полиса ОСАГО, перечисление денег и назначение встречи для передачи нового документа. Такой способ покупки используют водители, которые осознают, что покупают подделку.

Другие водители, которые становятся жертвами мошенников, полагают, что покупка в офисе по ожидаемой цене не может обернуться чем-то плохим. На деле же встречаются недобросовестные страховые агенты или брокеры, которые из-под полы торгуют страховыми полисами. Купить бланк ОСАГО с печатью можно и у них, но не всегда такой документ будет настоящим. Чаще всего мошенники располагают свои офисы вблизи отделений ГИБДД или МРЭО – этим они и подкупают автовладельцев.

Ответственность за нелегальное ОСАГО

В случае, если сотрудник ГИБДД при проверке документов усомнится в подлинности бланка ОСАГО и проверит его по базе, водитель с поддельным полисом может понести ответственность в соответствии с положениями Уголовного кодекса РФ. Но для этого правоохранительным органам придется доказать, что покупка фальшивки была намеренной, а водитель оказался недобросовестный. Наказание предусматривается двумя статьями УК РФ:

- Ст. 159 «Мошенничество». По статье может быть осуждено лицо или группа лиц, продававшая «левые» страховые полисы ОСАГО. В зависимости от квалификации преступления в виде наказания может быть применен штраф от 100 000 рублей, исправительные работы на срок от 1 года или лишение свободы на срок от 6 месяцев;
- Ст. 327 «Подделка, изготовление, сбыт...». Водитель, пойманный с подделкой, может быть осужден по части 3 этой статьи. Она предусматривает наказание в виде штрафа 80 000 рублей или исправительные работы на 2 года или арест сроком на полгода.

Левая страховка может стать причиной необходимости возмещать весь ущерб, нанесенный в ДТП. Страховая компания, от имени которой оформлен полис ОСАГО, не будет нести никакой ответственности за происшествие. Судебное разбирательство также не поможет водителю, ставшему виновником ДТП, поскольку страховщик с легкостью сможет доказать, что данный владелец автомобиля не мог приобрести подделку в этой компании.

Что делать, если купил поддельный полис ОСАГО?

О том, что у добросовестного водителя левый полис ОСАГО, он чаще всего узнает после ДТП с помощью сотрудников ГИБДД. Если этот водитель является виновником аварии, проблемы с выплатой возмещения будут у другого участника происшествия. Если он получит компенсацию от своего страховщика по прямому возмещению убытков, то виновник ДТП будет вызван в суд с требованием в порядке регресса компенсировать убытки. Если страховая откажет в выплате из-за ненастоящего бланка, то в суд будет обращаться не виновная в ДТП сторона.

Если водитель с поддельным полисом ОСАГО не будет виновником ДТП, то никаких последствий, кроме штрафа в 800 рублей по ст.12.37 КоАП РФ, для него может и не быть.

В случае обнаружения подделки такому автовладельцу стоит обратиться в РСА, чтобы проверить по базе свою страховку, а затем написать заявление в правоохранительные органы на продавца фальшивого бланка ОСАГО. И купить настоящий полис ОСАГО в проверенной страховой компании, чтобы впредь не попадать в такие ситуации.

Как вернуть деньги за фальшивое ОСАГО?

Вернуть деньги за фальшивый полис ОСАГО можно только одним путем – взысканием этих денежных средств с продавца бланка. Но для этого правоохранительные органы должны сначала его найти, затем должно состояться судебное разбирательство, после которого суд постановит возместить ущерб всем пострадавшим от действий мошенника. Исполнение наказания не всегда осуществимо, поскольку у продавца может не оказаться средств на счете, не будет имущества для продажи т.д. Так что вероятность вернуть потраченные на полис деньги очень невелика.

Заключение

Таким образом, всем автовладельцам, желающим приобрести полис ОСАГО, стоит внимательно подходить к процедуре, выбирать проверенные страховые компании, проверить действие их лицензии, а после покупки полиса ОСАГО обязательно проверить его подлинность по базе на сайте РСА. Только в таком случае водитель машины может быть уверен, что у него на руках подлинный бланк, который поможет получить ему страховое возмещение от компании после ДТП и не понести наказание за использование подделки по УК РФ».

7.2. О проблемах доступности е-ОСАГО

7.2.1. О проблемах оформления электронных полисов ОСАГО

Обратите внимание, что многие из приведенных материалов содержит ссылки на более ранние материалы, посвященные той же теме и представляющие интерес для ответа на вопросы кейса. Тем не менее, все материалы представляют точку зрения их авторов.

- **РБК – ОНФ выявил проблемы с покупкой полисов ОСАГО в регионах** **https://www.rbc.ru/finances/17/08/2018/5b7456119a79470f93a45c6f**

«Несмотря на усилия ЦБ по обеспечению доступности ОСАГО, проблемы с покупкой полисов не исчезли, следует из данных ОНФ. В ряде регионов купить е-ОСАГО невозможно. РБК опросил экспертов, как автовладельцу поступать в такой ситуации.

В целом ситуация с доступностью полисов ОСАГО в российских регионах к 2018 году улучшилась благодаря введению обязательной продажи полисов через интернет с 1 января 2017 года, но автовладельцы по-прежнему сталкиваются с проблемами, свидетельствуют данные ежегодного мониторинга рынка ОСАГО (есть у РБК), который проводит «Общероссийский народный фронт» (ОНФ).

Исследование в этом году состояло из двух этапов – пробного оформления электронной страховки е-ОСАГО на сайтах страховых компаний в 46 регионах во всех федеральных округах (всего было совершено 298 попыток провести покупку) и опроса 2345 автовладельцев, оформлявших ОСАГО в 2018 году.

«Ошибки» на сайтах с е-ОСАГО

Согласно данным ОНФ, почти в 60% случаях при попытке заключить договор ОСАГО через интернет у автовладельца возникли проблемы технического характера, а в четырех регионах ни одна попытка активистов фронта оформить е-ОСАГО не удалась. Неудачные попытки были зафиксированы в городах Черкесск (Карачаево-Черкесия), Владикавказ (Северная Осетия – Алания), Майкоп (Адыгея) и Улан-Удэ (Бурятия). Три из этих регионов входят в топ-10 самых убыточных по ОСАГО по итогам 2017 года, следует из статистики Российского союза автостраховщиков (РСА).

Среди проблем, которые фиксировали активисты ОНФ, – зависание сайта, сложности при регистрации, проблемы с получением кодов подтверждения, объявления о временной невозможности заключить договор ОСАГО. Как проблему пользователи фиксировали и переход с сайта страховой компании на сайт РСА, где гарантированно оформляется покупка полиса у компании, выбранной случайным образом. Замена страховщика часто не удовлетворяет клиента: предлагаемая страховая компания может быть малоизвестна или не иметь представительства в регионе страхователя, отмечают в ОНФ. Например, в Воронеже участнику исследования предложили заключить договор с новокузнецкой СК «Сибирский Спас», работающей в регионе через представителя, а автовладельцу из Зеленодольска (Татарстан) – в СК «Сервисрезерв» из города Коврова (Владимирская область).

В некоторых регионах владельцы мотоциклов (на них тарифы ОСАГО ниже автомобильных) сообщили о невозможности приобрести полис никаким способом. Так, мотоциклисты Кабардино-Балкарской Республики ездят за страховками в соседние регионы, говорится в мониторинге ОНФ.

Высокий процент «ошибок» при оформлении электронного полиса привязан к определенным регионам, утверждают авторы исследования, связывая это с политикой страховых компаний, направленной на сдерживание продаж ОСАГО в высокоубыточных регионах.

В РСА не согласны с выводами ОНФ. Проблема доступности полисов е-ОСАГО полностью решена, утверждают в союзе. «Нам поступают единичные жалобы на проблемы с покупкой полисов е-ОСАГО. Как правило, они вызваны скорее ошибками в заполнении данных со стороны страхователя, нежели какими-либо препонами со стороны страховых компаний», – пояснил представитель РСА. О снижении числа жалоб на доступность ОСАГО сообщили и в ЦБ – в первом полугодии 2018 года их число упало на 46%.

Убытки от ОСАГО

По данным РСА, за январь–июль 2018 года в России было заключено 10,7 млн договоров е-ОСАГО (около 40% от общего числа), что уже превышает число электронных полисов, приобретенных за весь 2017 год. Показатели гораздо скромнее в восьми регионах из топ-20 по убыточности для страховщиков – в Северной Осетии, Карачаево-Черкесии, Кабардино-Балкарии, Адыгее, Дагестане, Липецкой области, Краснодарском и Камчатском краях. Во всех перечисленных кавказских республиках, кроме Кабардино-Балкарии, уровень выплат по ОСАГО в 2017 году более чем вдвое превышал собранные страховые премии (с учетом расходов на судебные дела).

Система е-ОСАГО, которая должна была полностью искоренить проблему приобретения полисов в «токсичных» регионах и дать возможность выбрать любую

страховую компанию, в итоге работает так, что страховщики, не нарушая закон, могут избегать страхования нежелательных для них клиентов, говорит руководитель комитета по контролю качества страховых продуктов Объединения потребителей России Андрей Крупнов. «Эффективного инструмента контроля нет. Требования к работоспособности сайта страховщика недостаточно жесткие, и доказать умысел очень сложно», – отмечает он.

Страховщики не хотят развивать продажи в «токсичных» регионах из-за проблем тарификации и обилия недобросовестных автоюристов, говорит заместитель генерального директора «РЕСО-Гарантия» Игорь Иванов. «Тарифы ОСАГО не соответствуют частотности аварий в регионе, из-за этого коэффициенты неадекватно низкие, а если в регионе орудуют еще и автоюристы, то, очевидно, у компании не будет горячего желания там работать», – отмечает он.

На высокую убыточность в регионе, из-за которой страховщики не хотят продавать там свои полисы, влияют и многие другие факторы, такие как природно-климатические условия, состояние дорог, плотность дорожного движения, добавляет Крупнов.

При отсутствии выбора

У автомобилистов в проблемных регионах нет возможности выбора страховщика, говорят опрошенные РБК эксперты. Из-за того, что при оформлении полиса на сайте клиент из «токсичного» региона часто сталкивается с техническими «ошибками», у него нет иного выбора, кроме как оформить полис там, где ему предложит система случайного распределения, отмечает Андрей Крупнов.

Если вообще не получается купить электронный ОСАГО, то основной способ решить проблему – идти в офис страховой компании, говорит председатель правления Международной конфедерации обществ потребителей (КонфОП) Дмитрий Янин. Там чаще всего подстерегает такая страховая уловка, как отказ в заключении договора ОСАГО без покупки доппродукта, поэтому надо покупать вместе с ОСАГО этот «довесок», а потом от него отказываться, пока действует «период охлаждения» (время отказа от страхового продукта), советует эксперт.

«Если ОСАГО не продают и с дополнительными продуктами, последний вариант – до посинения заполнять электронный полис», – отметил Янин, добавив, что КонфОП известен случай, когда владелец мотоцикла заполнял данные на полис е-ОСАГО в течение двух дней.

Можно также пожаловаться в РСА и ФАС, отмечает управляющий партнер коллегии адвокатов «Старинский, Корчаго и партнеры» Владимир Старинский. Так как страховые компании не имеют права отказать в такой услуге без законных оснований, то компанию обяжут оформить полис без дополнительных услуг и наложить штраф на страховую, говорит юрист, добавляя, что желательно записывать процедуру покупки полиса на диктофон или на видео.

Все незаконные действия страховых компаний можно обжаловать в суде – вопрос лишь в представлении доказательств нарушенного права, то есть в наличии письменного отказа в полисе ОСАГО (компании чаще всего отказывают устно), говорит адвокат юридического департамента «НЮС Амулекс» Александр Домнин. Правила страхования декларируют, что заключать договор клиент имеет право с любой страховой компанией, при этом «страховщик не вправе отказать в заключении договора». Необходимо, покупая

ОСАГО в офисе, зафиксировать свое заявление на заключение договора страхования. С электронным ОСАГО сложнее: страховщика нельзя обвинить в плохом функционировании сайта и посчитать это за отказ оформлять ОСАГО, резюмирует Домнин.

Что показал опрос автовладельцев

Проведенный ОНФ опрос автовладельцев, заключавших договоры не через интернет, а в офисах страховых компаний, выявил массовое навязывание страховыми компаниями дополнительных услуг – 49,6% опрошенных сталкивались с этим. Среди мотоциклистов эта доля еще выше – 56%. Среди навязанных дополнительных услуг – платный техосмотр и дополнительные страховые продукты, в том числе страхование жизни, имущества и пр.

Вторая по частоте проблема – невозможность заключить договор из-за технических проблем у страховщика (25,8% респондентов). Среди владельцев такси и мотоциклов эта доля еще выше – 30,0 и 28,8% соответственно.

Замыкают тройку претензий автовладельцев (20,9%) длинные очереди. Среди владельцев такси доля жалующихся на них наиболее высока – 28,1%. В частности, активисты из Хабаровска сообщили, что очередь «по предварительной записи» может доходить до трех недель, из-за чего люди, купившие новый автомобиль, не могут зарегистрировать его в ГИБДД в десятидневный срок, как того требует закон, и вынуждены платить штраф в размере 1,5 тыс. руб».

Материалы блога содержат много полезной информации по вопросам кейса и время от времени обновляются:

- **Блок Кулика Ильи – Причины, по которым не получается оформить электронное ОСАГО: технические сбои, хитрости компаний, законные способы + что делать**
  http://kulikavto.ru/osago/ne-mogu-zastrahovat-avtomobil-po-osago-onlajn-prichiny-ulovki-kompanij-chto-delat.html

«Все чаще в интернете встречаются фразы вроде: «не могу застраховать автомобиль по ОСАГО онлайн», «выдает необоснованную ошибку», «виснет страница оформления», «не могу различить капчу» и т. п.

Сегодня я расскажу, почему страховые компании могут целенаправленно саботировать нововведения в законе об обязательной электронной страховке. Действительно ли в системе технический сбой или вас просто игнорируют. Как с этим бороться и куда можно пожаловаться страхователям. Поехали!

Содержание

1. Невозможность страхования по ОСАГО онлайн
2. Законодательная база оформления е-ОСАГО и ответственность страховых компаний
    1. Что грозит страховой компании за отказ оформить ОСАГО в электронном виде
3. Каким образом подобные проблемы могут быть преодолены страхователем
4. Как и для чего страховые компании умышленно ограничивают возможность оформления е-ОСАГО
5. Возможные технические причины, не позволяющие оформить е-ОСАГО

1. Возможные технические причины со стороны страхователя
2. Возможные технические причины со стороны страховщика

6. Что делать страхователю при возникновении проблем с оформлением е-ОСАГО и куда можно пожаловаться
7. Самые убыточные регионы по информации на февраль 2018
8. Информация к размышлению
9. Заключение»

- **На сайте юридических консультантов Правовой центр https://pravovoi.center/avtoyurist/avtoctrahovanie/osago/elektronnyj/ne-poluchaetsya-kupit-polis-onlajn.html приведены следующие проблемы, сопровождающие онлайн процедуру приобретения полиса:**

«Первая проблема связана с невозможностью купить электронный полис из-за ошибки, которая всплывает на сайте. Если вы не можете застраховать автомобиль онлайн, то для начала необходимо удостовериться в том, что вы правильно заполнили основные поля по требованию сайта. Если вами была допущена ошибка, то сайт скорее всего, запретит вам осуществить покупку без исправления. Обычно, хорошо функционирующие сайты отмечают красным цветом поля, где были допущены недочеты. В случае, если данные были введены правильно, но оплата все равно не осуществляется, то это значит, что проблема в электронном ресурсе.

Вторая проблема связана со страхом клиентов компании взлома банковской карты после оплаты полиса. К сожалению, риск раскрыть свои данные при покупке ОСАГО точно такой же, как и в любом интернет-магазине. Если в программу было запущено вирусное приложение, то оно сможет считать информацию с вашего счёта, и ваша карта перестанет вам принадлежать.

Следующая проблема связана с тем, что электронный полис ОСАГО не приходит на почту после оплаты. Такая неприятная ошибка зачастую связана с тем, что ресурсу необходимо некоторое время, чтобы ввести новые данные в свою базу, а затем уже переслать готовый бланк по почте.

Иногда сотрудники ГИБДД отказываются принимать составленный вами электронный полис ОСАГО, который граждане обязуются передавать для проверки в соответствии с статьей 2 п.1.1 ПДД. Хотя, по закону достаточно всего лишь распечатать этот документ и возить с собой в машине (ФЗ № 40, ст.15 п.7.2). Сотрудники ГИБДД могут требовать наличие соответствующей печати и бланка страховой компании в подлинном виде (о том, как пользоваться документом и что предъявлять инспектору ГИБДД для проверки, узнайте тут).

Еще одна проблема связана с тем, что на сайте нет пункта меню «купить электронное ОСАГО». К сожалению, возможностью осуществлять продажу электронных документов ОСАГО пользуются далеко не все фирмы-страховщики, хотя Федеральный закон об ОСАГО обязывает все компании добавить такую услугу в основной перечень. Около 50% страховщиков осуществляют продажу полисов при помощи Интернета. Поэтому, даже на сайте достаточно популярных страховых может отсутствовать функция приобретения электронного документа. В таком случае, гражданину ничего не остаётся, как самостоятельно явиться в офис компании, и приобрести полис ОСАГО лично».

Блоги автовладельцев о проблемах покупки электронного полиса:

- **ProСтрахование – Электронное ОСАГО онлайн - это РАЗВОД! А нас держат за идиотов**
  https://proins.ru/avtostrakhovanie/osago/1140-elekronnoe-osago-eto-razvod-a-nas-derzhat-za-idiotov

> «Не могу оформить электронный полис ОСАГО, можно сутками тыкать по кнопкам пытаясь оформить полис. Раз за разом вводить информацию, утром, в обед и вечером, можете встать даже ночью, но электронное ОСАГО Вы НЕ ОФОРМИТЕ! И даже не надейтесь...».

- **4memo.ru – Купил Е-ОСАГО с третьей попытки: РЕСО – Ингосстрах – Тинькофф**
  http://4memo.ru/e-osago

> «Так получилось, что мне пришлось опробовать оформление полиса на сайтах трех страховщиков: РЕСО, Ингосстрах, Тинькофф. Далее идет получившийся сам собой краткий обзор-сравнение процедуры оформления у перечисленных страховщиков.
>
> Содержание
>
> 1. Попытка получить Е-ОСАГО у РЕСО;
> 2. Попытка купить Е-ОСАГО в Ингосстрахе;
> 3. Попытка купить полис Е-ОСАГО в Тинькофф Страхование».

7.3. Об изменениях регулирования ОСАГО

7.3.1. О текущих изменениях нормативной базы

- **Российская газета – ЦБ изменил порядок оформления электронных полисов ОСАГО**

> «Банк России изменил порядок покупки полисов ОСАГО через интернет, чтобы снизить возможность страховщиков заблокировать или затруднить оформление полисов на своих сайтах.
>
> Банк России установил, что ключ простой электронной подписи может состоять только из латинских букв и цифр. "Это позволит избежать ситуации, когда автовладелец не может зарегистрироваться в личном кабинете на сайте страховщика из-за того, что в ключе используются схожие по написанию русские и латинские буквы", - говорится в сообщении регулятора.
>
> Документом определены случаи, когда электронный договор ОСАГО может заключаться через сайт Российского союза автостраховщиков (так называемая система гарантирования). Страховщик при этом будет обязан фиксировать переход страхователя в систему гарантирования в своей информационной системе для контроля правомерности использования данной системы, в том числе со стороны Банка России.
>
> Обязанность страховщиков обеспечивать заключение договоров ОСАГО в электронном виде введена с начала прошлого года. В первом квартале этого года (последние доступные данные) каждый четвертый полис был оформлен через интернет. Вместе с тем для многих страховых компаний работа с ОСАГО по-прежнему

является убыточной: в целом по рынку, согласно расчетам Банка России, коэффициент убыточности ОСАГО составил 67,8 процента.

Одновременно для борьбы с мошенничеством со стороны владельцев автомобилей установлены требования к отсканированным копиям документов (они должны иметь формат pdf, jpg, jpeg, bmp, png, tif, gif, размер - не более 2 Мб), которые они загружают на сайт страховщика, введено правило, что договор е-ОСАГО не может вступать в силу ранее трех дней с даты его заключения, а также определено, что на один номер телефона может быть зарегистрирован только один личный кабинет страхователя на сайте страховщика.

По итогам первого квартала Банк России отмечал еще большее сокращение средней премии по договорам ОСАГО с физическими лицами (минус 4,4 процента, до 5,6 тысячи рублей), связывая это с мошеннической деятельностью при оформлении е-ОСАГО, нацеленных на искажение данных о страхователе для получения более низкого коэффициента.

Изменения вступят в силу по истечении 10 дней со дня опубликования на сайте Банка России».

- **Ведомости – ЦБ изменил правила оформления электронного ОСАГО**
  https://www.vedomosti.ru/finance/news/2018/08/24/778960-tsb

«Минюст России зарегистрировал указание Центробанка России об изменениях правил оформления электронного полиса ОСАГО. Копия документа размещена на официальном сайте регулятора. Изменения вступят в силу через 10 дней с момента их опубликования на сайте ЦБ.

Они позволят упростить процесс заключения электронного договора ОСАГО, «сделают сервис электронных продаж более удобным для автовладельцев», считают в ЦБ. Нововведения также будут препятствовать совершению злоупотреблений участниками страхового рынка.

Для повышения доступности электронных полисов ОСАГО ЦБ постановил, что ключ простой электронной подписи будет состоять теперь только из латинских букв и цифр. «Это позволит избежать ситуации, когда автовладелец не может зарегистрироваться в личном кабинете на сайте страховщика из-за того, что в ключе используются схожие по написанию русские и латинские буквы», - объяснили в ЦБ.

Документом также определены случаи, когда электронный полис может быть заключен через сайт Российского союза автостраховщиков, так называемую систему гарантирования. ЦБ обязал страховую компанию фиксировать переход страхователя в систему гарантирования в своей информационной системе для контроля правомерности использования данной системы, в том числе со стороны регулятора.

Для снижения риска мошенничества введены новые требования к отсканированным копиям документов, которые страхователь загружает на сайт страховщика. В частности, копии документов должны иметь графический формат (pdf, jpg, jpeg, bmp, png, tif, gif), размер одного файла должен быть не более 2 Мб, копия должна содержать графическое изображение всех реквизитов оригинального документа, быть доступной к просмотру и копированию неограниченным количеством лиц.

Также ЦБ ввел правило, согласно которому электронный полис ОСАГО не может вступать в силу ранее трех дней с даты его заключения. Помимо этого, на один номер телефона может быть зарегистрирован только один личный кабинет страхователя на сайте страховщика.

В России с 1 января 2017 г. все страховые компании обязали продавать электронные полисы ОСАГО. Соответствующие поправки в закон об автогражданской ответственности Госдума одобрила летом 2016 г. До 1 января 2017 г. страховые компании предоставляли такую услугу добровольно. Чтобы заключить договор онлайн, нужно завести личный кабинет на сайте страховой компании, заполнить заявление и оплатить полис банковской картой. После этого страховщик направляет клиенту страховой полис по электронной почте и размещает в его личном кабинете на сайте».

- **РБК – Центробанк изменил правила оформления е-ОСАГО**
  https://www.rbc.ru/finances/24/08/2018/5b7fb2c29a7947931b791321

«Изменения внесены для упрощения процесса оформления электронных договоров ОСАГО, а также для борьбы с мошенническими схемами, объяснил ЦБ. С проблемами покупки полисов чаще сталкиваются жители регионов с высокой убыточностью ОСАГО

Центробанк изменил правила оформления электронных полисов ОСАГО, сообщается на сайте регулятора. Изменения вступят в силу по истечении десяти дней.

Новые правила позволят упростить процесс заключения электронного договора ОСАГО и сделать его более удобным для клиентов, а также лучше защитить всех участников страхового рынка, рассчитывают в ЦБ.

Исключить отказы

Чтобы повысить доступность полисов е-ОСАГО, ЦБ установил, что ключ простой электронной подписи может состоять только из цифр и латинских букв. «Это позволит избежать ситуации, когда автовладелец не может зарегистрироваться в личном кабинете на сайте страховщика из-за того, что в ключе используются схожие по написанию русские и латинские буквы», – поясняет ЦБ.

Ранее ОНФ («Общероссийский народный фронт») провел ежегодное исследование, целью которого стало выявление проблем с оформлением и доступностью электронных полисов в российских регионах. Согласно данным ОНФ, почти в 60% случаев при попытке заключить договор ОСАГО через интернет у автовладельца возникали проблемы технического характера, а в четырех регионах ни одна попытка активистов ОНФ оформить е-ОСАГО не удалась. Речь идет о проблемных для страховщиков регионах, где убыточность ОСАГО высока и страховые компании не заинтересованы в привлечении клиентов.

Также ЦБ вводит для страховщиков новые требования: при заключении страхового договора через сайт Российского союза автостраховщиков (РСА, система гарантирования) страховщик должен контролировать «правомерность использования» данной системы, в том числе со стороны Банка России. Для этого страховые компании будут фиксировать каждый переход в систему гарантирования на своей стороне.

Как писал ранее РБК, среди основных проблем при оформлении полиса е-ОСАГО страхователи отмечают именно переход с сайта страховой компании на сайт РСА, где

гарантированно оформляется покупка полиса у компании, выбранной случайным образом. Замена страховщика часто не удовлетворяет клиента: предлагаемая компания может быть малоизвестна или не иметь представительства в регионе страхователя, отмечают в ОНФ. Например, в Воронеже участнику исследования предложили заключить договор с новокузнецкой СК «Сибирский Спас», работающей в регионе через представителя, а автовладельцу из Зеленодольска (Татарстан) – в СК «Сервисрезерв» из города Коврова (Владимирская область).

Против мошенников

Центробанк установил требования к электронным копиям документов, которые клиенты е-ОСАГО загружают на сайт страховой компании, и определил, что договор со страховой компанией может вступить в силу только через три дня после его заключения. Кроме того, к одному телефонному номеру может быть привязан только один личный кабинет клиента страховой компании. Сейчас на один номер можно регистрировать неограниченное число личных кабинетов.

Эти меры призваны перекрыть распространенную схему мошенничества на рынке ОСАГО, их проработку ЦБ и Российский союз автостраховщиков (РСА) обсуждали еще в октябре прошлого года, писал РБК.

То, что электронный полис будет вступать в силу через три дня после оформления, поможет избежать ситуаций, когда автовладелец, попавший в ДТП и не купивший полис ОСАГО, оформляет его в электронном виде прямо на месте события, заявили РБК в РСА. Возможность регистрировать на один номер телефона только один личный кабинет поможет в борьбе с недобросовестными посредниками, оформляющими полисы на других лиц, считают в РСА. Ряд технических новаций – изменение ключа шифрования, требования к файлам и другие позволят упростить процедуру заключения электронного полиса ОСАГО, согласны в РСА.

Как работает схема мошенничества

Водитель обращается с просьбой оформить полис е-ОСАГО к компании-посреднику, та при заполнении заявки на полис вписывает неверные данные об автомобиле, регионе или мощности, которые значительно занижают стоимость полиса, однако данные идентификационного номера транспортного средства (ТС) и его регистрационный номер (VIN) вписывает верно. Затем в фоторедакторах данные о марке машины, регионе и прочее изменяются уже на верные, а полис, оформленный дешево на подставные данные, после корректировки распечатывается и продается по реальной цене ничего не подозревающему водителю, а разницу мошенники кладут в карман. При наступлении страхового случая из-за расхождения данных в базе страховщика и бумажном полисе выплат водитель не получает.

Изначально электронное ОСАГО вводилось для защиты от «уличных брокеров» и для удобства клиентов: чтобы автовладелец мог оформить полис не выходя из дома. Реальность же такова, что некоторые плохо владеют компьютером или не хотят тратить время на заполнение полиса, поэтому человек ищет альтернативный способ и обращается к «помощникам» на стороннем сайте, которые могут оказаться мошенниками. Мошенниками могут выступать в основном посредники, которые предлагают в интернете оформить за водителя полис е-ОСАГО. Сейчас работа таких сайтов никак не урегулирована.

С полным текстом названного выше документа Банка России Указание Банка России от 14.11.2016 N 4190-У (ред. от 15.02.2018) "О требованиях к использованию электронных документов и порядке обмена информацией в электронной форме при осуществлении обязательного страхования гражданской ответственности владельцев транспортных средств" можно ознакомиться по ссылке http://legalacts.ru/doc/ukazanie-banka-rossii-ot-14112016-n-4190-u-o-trebovanijakh/».

7.3.2. О перспективах реформирования

Здесь представлены как некоторые материалы о направлениях реформирования ОСАГО, так разные взгляды на обсуждаемые перспективы.

- **Гарант – РСА: большинство автомобилистов поддерживают идею либерализации тарифов ОСАГО**
  http://www.garant.ru/news/1152402/

«По результатам исследования холдинга Ромир, проведенного в ноябре, 53% автомобилистов выступают за либерализацию ОСАГО. Об этом сообщил на состоявшейся на прошлой неделе пресс-конференции президент Российского союза автостраховщиков (РСА) Игорь Юргенс. Он отметил, что такое позитивное отношение к установлению индивидуальных тарифных коэффициентов связано с тем, что эти нововведения будут учитывать особенности вождения каждого автомобилиста, что позволит неаварийным и аккуратным водителям платить значительно меньше.

В частности, принимая решение по тарифу, страховщик будет учитывать не только характеристики автомобиля, цели его использования и вид собственника, но и манеру вождения водителя. То есть предполагается, что страховщиком может быть установлено специальное устройство (телематическое оборудование), при помощи которого будет осуществляться мониторинг основных показателей движения машины. Таким образом у страховой компании появится возможность скорректировать размер тарифа в зависимости от стиля вождения клиента. Сегодня такой способ экономии страховщики предлагают автомобилистам только при оформлении полиса КАСКО.

"Предполагается, что должен сформироваться конкурентный рынок, где сам водитель будет выбирать страховую компанию в зависимости от тарифов, которые она предлагает, и страховые компании будут "бороться" за неаварийных водителей, предлагая им низкие тарифы", – поясняет Игорь Юргенс. Напомним, что сейчас "вилка" тарифов по ОСАГО устанавливается Банком России (ч. 1 ст. 9 Федерального закона от 25 апреля 2002 г. № 40-ФЗ "Об обязательном страховании гражданской ответственности владельцев транспортных средств"; далее – закон об ОСАГО).

Эксперты также отметили, что установление индивидуальных тарифных коэффициентов позволит решить в том числе проблемы, связанные с мошенничеством при продаже полисов в регионах. Игорь Юргенс рассказал, что, например, в Крыму за 9 месяцев 2017 года накладные расходы страховых компаний по выплатам составили 135,2 млн руб., а в прошлом году за этот же период они не превышали 15,7 млн руб. По его словам, это связано с тем, что если в Москве территориальный коэффициент, с учетом которого осуществляется расчет стоимости полиса ОСАГО, равен 2, то в Крыму он втрое ниже – 0,6 (указание Банка России от 19 сентября 2014 г. № 3384-У). Таким образом с помощью "автоюристов" водители оформляют электронную страховку в регионах, для которых

установлены самые низкие коэффициенты, но при этом указывают регистрационный номер и VIN (идентификационный номер транспортного средства) автомобиля реального покупателя полиса. По словам экспертов, оперативно проверить подлинность такого полиса практически невозможно, так как даже сотрудники ГИБДД при проверке полиса ОСАГО проверяют данные о госномере автомобиля и номере VIN, а на несовпадение данных по региону и места регистрации владельца машины обычно не обращают внимания. "Для тех регионов, где ситуация с мошенничеством и убыточностью по ОСАГО оценивается как "желтая зона", должна быть предусмотрена возможность страховщика самостоятельно устанавливать ставку тарифа", – считает Игорь Юргенс.

По словам руководителя департамента количественных исследований холдинга Ромир Светланы Поликаниной, с такой позицией согласны в том числе и водители. "Отношение к различного рода мошенническим схемам с ОСАГО ("автоподставами", имитациями ДТП, продаже поддельных полисов и т. д.) у автомобилистов отрицательное. Респонденты видят в этом большую проблему, требующую скорейшего решения. Участники опроса считают, что из-за мошенников страдают дисциплинированные водители и видят необходимость ужесточать ответственность за любое мошенничество в сфере автострахования", – отметила эксперт.

Напомним, что в ходе либерализации ОСАГО предлагается также увеличить срок страхования по ОСАГО до трех лет (по соглашению сторон), при этом тариф не будет меняться на протяжении всего срока страхования. Кроме того, обсуждается увеличение размера возмещения ущерба до 2 млн руб. (сегодня – до 500 тыс. руб.). Эти и другие нововведения пока находятся на стадии обсуждения в заинтересованных ведомствах.

В заключение Игорь Юргенс отметил, что текст поправок в закон об ОСАГО требует тщательной проработки и предполагается, что закон вступит в силу с 1 июля 2018 года».

- **ПРАЙМ – Рост тарифов ОСАГО: мошенников станет больше?**
  https://1prime.ru/business/20180615/828934708.html

«Центробанк РФ опубликовал проект указаний о предельных значениях тарифов ОСАГО. Новый порядок страхования предусматривает увеличение коридора базового тарифа по полисам ОСАГО на 20% вниз и вверх от нынешней стоимости. Исключение составят мотоциклы и легковые автомобили юридических лиц, в этих случаях верхняя граница вырастет на 10,9% и 5,7% соответственно.

Закон об ОСАГО позволяет ЦБ менять тарифы не чаще одного раза в год. Центробанк дважды воспользовался этим правом, увеличив тарифы. Последний раз изменения произошли в апреле 2015 года.

В настоящее время базовый тариф для физических лиц составляет от 3,431 тысячи до 4,119 тысячи рублей. Согласно новым указаниям, базовые значения тарифа составят от 2,746 тысячи до 4,942 тысячи рублей.

В сообщении регулятора отмечается, что данный законопроект – первый шаг по изменению системы тарифов в ОСАГО.

Новые тарифы ОСАГО приведут к подорожанию полисов страхования, по крайней мере, для определенной части автомобилистов и в некоторых регионах, считают эксперты,

опрошенные «Прайм». При этом рост страховых взносов может быть «компенсирован» падением числа застрахованных автолюбителей.

Убыточное ОСАГО

Выступая недавно в Совете Федерации председатель Банка России Эльвира Набиуллина, назвала ОСАГО «наиболее проблемным» видом страхования. По ее словам, проблемы на рынке ОСАГО накапливались в течение долгого времени, и в ряде регионов ОСАГО стало убыточным.

В Российском союзе автостраховщиков (РСА) говорят, что либерализации тарифов ОСАГО позволит рынку достигнуть хотя бы нулевой убыточности. Там подчеркивают, что за последние семь лет размер средней премии увеличился в 2,3 раза, а средней выплаты почти в 3,2 раза, что негативно сказалось на финансовой устойчивости страховщиков.

Средняя выплата по ОСАГО в 2017 году выросла на 10% и составила 75,763 тысячи рублей, а средняя премия упала на 4% – до 5,819 тысячи рублей. При этом, в прошлом году страховщики собрали с автовладельцев 228 млрд рублей, а выплатили по страховым случаям 181 млрд рублей.

Учитывая разницу между страховыми премиями и выплатами по ОСАГО, в прошлом году лидеры рынка заработали на автостраховках: «РЕСО-Гарантия» – 14 млрд рублей, «Альфа-Страхование» – 10 млрд, СОГАЗ – около 8 млрд, Ингосстарх – 6 млрд, ВСК – 5 млрд.

Убытки в 24,5 млрд рублей понес только Росгосстрах.

ПОДОРОЖАЕТ ЛИ ПОЛИС?

Эксперты разошлись во мнении о подорожании полисов ОСАГО после введения новых тарифов.

«По верхней планке – на 20%, подорожают полисы тех клиентов, которых страховые компании быть может не очень хотят у себя видеть. Это проблемные водители с высокой аварийностью, небольшим стажем и из проблемных регионов, где орудуют так называемые «автоюристы», и где очень высокий уровень мошенничества», – считает управляющий директор по страховым рейтингам «Эксперт РА» Алексей Янин.

По его словам, цена полиса ОСАГО может снизиться в некоторых регионах, например, в Москве и ряде крупных городов, где «нормальная ситуация с убыточностью страховых компаний по ОСАГО». Кроме того, цена полиса может снизиться для опытных безаварийных водителей, считает эксперт.

«Водителям, которым не повезло жить в проблемном регионе, видимо, практически автоматически придется столкнуться с повышением стоимости ОСАГО, а безаварийным водителям с большим опытом вождения, живущим в непроблемных регионах, стоимость полиса вполне может снизиться», – говорит Янин.

Руководитель управления страховых рейтингов НРА Татьяна Никитина считает, что для большинства автовладельцев стоимость полиса увеличится. По крайней мере, в первое время страховщики будут работать по верхней границе тарифного коридора. Средняя стоимость полиса вырастет с 5,8 тысячи до 7 тысяч рублей. Для мотоциклов, мотороллеров и легковых автомобилей юридических лиц верхняя граница снизится, говорит эксперт.

По мнению Янина, страховщики не смогут вступить в сговор и выставить единую цену полиса, поскольку компаний на рынке ОСАГО работает много и они между собой конкурируют. «Поэтому, если кто-то из страховщиков будет ставить неоправданно высокие цены, всегда найдутся участники рынка, которые поставят цены ниже и, соответственно, будут привлекать клиентов к себе», – говорит Янин.

Эксперты считают, что изменение базовых тарифов приведет к росту страховых премий по ОСАГО. В проблемных регионах взносы вырастут сильнее – по верхней планке в 20%. Как сложится ситуация в других регионах, пока предсказать трудно. «Политика разных компаний по тарифам может разойтись, поскольку у них появится больше свободы, и каждая страховая компания будет сама рассчитывать стоимость полисов», – считает Янин.

ПОДОРОЖАНИЕ ОСАГО УМЕНЬШИТ ЧИСЛО ЗАСТРАХОВАННЫХ

Рост стоимости полиса ускорит падение спроса на ОСАГО, активизирует рынок подделок и вызовет всплеск страхового мошенничества, предупреждают специалисты.

По данным РСА, пик количества заключенных договоров ОСАГО приходился на 2013 год, когда страховщики заключили 42,7 млн договоров. В 2017 году этот показатель снизился до 39,2 млн. В РСА объясняют снижение тем, что автовладельцы эксплуатируют транспортные средства без договора ОСАГО или пользуются поддельными полисами. Из-за этого страховые компании недобирают примерно 20 млрд рублей в год.

Эта тенденция сохраняется и в этом году, несмотря на рост продаж автомобилей. По данным ЦБ, число проданных полисов ОСАГО сократилось в первом квартале на 1,3%. Страховые премии уменьшились на 4,6%, до 46 млрд рублей.

Рост тарифов ОСАГО может привести к демпингу и мошенничеству на рынке, предупреждают эксперты. «Если появится недобросовестная компания, которая захочет «попылесосить» рынок, она поставит цену полиса по нижней планке и все автомобилисты пойдут страховаться к ней. Затем компания может исчезнуть с деньгами автомобилистов. Такая опасность существует», – говорит Янин.

Ситуацию может изменить более индивидуальный подход страховщиков к автолюбителям. Никитина видит положительные моменты в новом проекте ЦБ в ориентации на индивидуализацию тарифов: увеличении числа градаций для коэффициента «возраст-стаж» с 4 до 50, а также в том, что коэффициент бонус-малус будет устанавливаться на год (сейчас меняется после каждой аварии), а страховая история будет закреплена за водителем, а не транспортным средством».

- **Центральный Банк Российской Федерации – Индивидуальный тариф ОСАГО: первый шаг**
  http://www.cbr.ru/press/event/?id=2271#highlight=%D0%BE%D1%81%D0%B0%D0%B3%D0%BE

«Совет директоров Банка России утвердил указание о предельных размерах базовых ставок и коэффициентов страховых тарифов по ОСАГО, а также о порядке их применения страховщиками при определении страховой премии. В ближайшее время документ будет направлен на регистрацию в Министерство юстиции.

Банк России совместно с Минфином подготовил комплекс инициатив по ОСАГО. Они направлены на повышение доступности полисов ОСАГО и переход к системе, где каждый водитель платит сам за себя, а тариф является справедливым и индивидуальным

для каждого автолюбителя. Принятое указание является первым этапом реализации разработанных мер.

Указание вводит более гибкую систему коэффициента возраст-стаж (КВС) с более детальной градацией ступеней (58 вместо действующих четырех). По итогам проведенных актуарных расчетов для опытных водителей старшего возраста КВС будет снижен, а для молодых и неопытных – повышен. Таким образом, для наиболее рискованного сочетания возраста и стажа коэффициент будет равен 1,87; для наименее рискованного сочетания (автолюбители старше 59 лет со стажем более 3 лет) коэффициент будет фактически в два раза меньше – 0,93, что создаст льготные условия для лиц пенсионного возраста. Это позволит сделать цену полиса более индивидуальной.

Документ предусматривает переход к простой и понятной системе присвоения коэффициента бонус-малус (КБМ). КБМ будет назначаться водителю раз в год 1 апреля и в течение года пересчитываться не будет. Если на 1 апреля 2019 года у автовладельца в системе АИС РСА будет числиться несколько коэффициентов бонус-малус, то ему будет присвоен самый низкий из них. Такой подход позволит исключить случаи задвоения КБМ, а также снизит риск ошибок и злоупотреблений при его применении. Новая система КБМ закрепляет страховую историю за водителем и предполагает отказ от ее обнуления при перерыве в вождении: все накопленные скидки будут сохраняться.

Юридическому лицу будет присваиваться единый для всех машин в автопарке КБМ, что существенно упростит проведение конкурсов на заключение договоров ОСАГО.

Кроме того, предусматривается расширение тарифного коридора базовых ставок страхового тарифа на 20% вниз и 20% вверх.

Предлагаемые изменения не позволят в полной мере уйти от уравнительного ценообразования в ОСАГО и перейти к индивидуальному тарифу для каждого водителя, поскольку для этого необходимо изменить закон. Но тем не менее они создадут возможности для применения более дифференцированного подхода к установлению тарифов и сделают систему ОСАГО более справедливой».

- **Udm-info – Реформа ОСАГО сделает тарифы индивидуальными**
  https://udm-info.ru/news/autolife/23-11-2018/reforma-osago-sdelaet-tarify-individualnymi

«И будет выгодна аккуратным водителям.

Реформа ОСАГО реализация которой намечена в следующем году сделает тарифы максимально прозрачными и индивидуальными.

Эксперты ЦБ России убеждены, что реформа сделает отношение к добросовестным водителям со стороны страховщиков более понятным и лояльным. Причем, вне зависимости от места проживания, региона и муниципалитета. Кроме того, аккуратные участники дорожного движения смогут рассчитывать на существенное снижение тарифа, лихачам же придется раскошелиться.

Udm-info выяснил, какие законодательные нововведения сейчас обсуждаются в Центробанке и Минфине и как они отразятся на рядовых водителях.

Региональный коэффициент останется в прошлом

Сейчас стоимость полиса ОСАГО рассчитывается по жесткой формуле, которая учитывает несколько коэффициентов: возраст и стаж водителя, мощность автомобиля, количество аварий на этом автомобиле, а также так называемый территориальный коэффициент, то есть наценка или снижение стоимости полиса в зависимости от региона и населенного пункта, в котором зарегистрирован автовладелец. Этот набор коэффициентов не менялся с 2003 года и на сегодня уже устарел.

Первое, что предлагается изменить, это убрать территориальный коэффициент. То есть на цену полиса уже не будет влиять место жительства водителя.

Сейчас в зависимости от региона и населенного пункта стоимость автогражданского страхования может вырастать в 2 раза или снижаться до 40%. Например, жители городов Удмуртии платят за полис в том числе повышающий территориальный коэффициент 1,2. А в малых населенных пунктах края действует понижающий коэффициент 0,7.

Уфинец Александр сетует: при переезде из Увы в Ижевск его ожидал неприятный сюрприз. Купив в столице Удмуртии другой автомобиль и приобретая полис ОСАГО он был неприятно удивлен коэффициентом, который начислила страховая компания. Его величина значительно превышала прежнюю. Стиль вождения, аварийность, стаж… Все это оказалось не важным. Обидно!

В Центробанке согласны, ситуация ненормальная.

«Действующую сегодня систему тарифов сложно назвать гибкой, поскольку она приводит к уравниловке всех водителей вне зависимости от их опыта и стажа, аварийности и поведения на дороге. Возьмем, к примеру, двух водителей с автомобилями Lada Granta мощностью 87 лошадиных сил из Мурманска. У одного стаж 3 года, а у второго – 20 лет. Стоимость полиса для них будет одинаковой – 9 512 рублей, хотя по справедливости, как показывают расчеты, первый из них должен платить 29 134, а второй – 7 847 рублей. Неопытный водитель из Курганской области платит почти в 2 раза меньше безаварийного водителя Челябинска», - говорит директор департамента страхового рынка Банка России Филипп Габуния.

Жесткая система тарифов была хороша на момент запуска ОСАГО, добавляет эксперт. Тогда она не позволяла страховым компаниям завышать цены и делала полис доступным для большинства автомобилистов. Но со временем формула расчета полиса стала уравнительной, а иногда и попросту несправедливой, когда аккуратный водитель платит за лихача.

В новом варианте планируется иной подход. Предлагается дать страховым компаниям право использовать дополнительные параметры при формировании стоимости полиса и устанавливать для каждого водителя индивидуальный тариф внутри тарифного коридора. В эти критерии могут входить индивидуальные показатели водителя: то, как он водит, как часто выезжает, сколько раз попадал в аварию или платил штрафы ГИБДД и прочее. Тогда профессиональные водители, которые зарабатывают на своем авто, а также лихачи и нарушители будут платить больше, а аккуратный и опытный водитель, который раз в неделю выезжает на своей машине на дачу, соответственно, будет платить меньше.

Мощность авто становится не определяющим фактором

Планируется изменить подходы и вопросе учета мощности автомобиля. Так в старой редакции при мощности двигателя 121 до 150 лошадиных сил цена полиса вырастает сразу на 40%, что в деньгах – более 2 тысяч рублей. А при 151 лошадиной силы под капотом водитель платит уже на 60% больше, это почти 3,5 тысячи рублей надбавки. При этом времена, когда машина мощностью 120 «лошадок» считалась спортивной, ушли в прошлое.

Сейчас большинство легковых машин на дорогах страны имеют мощность от 71 до 100 лошадиных сил. И для них до сих пор действует повышающий коэффициент за мощность. В новой системе расчета предлагается убрать этот коэффициент из стоимости полиса.

Страховые компании и рады бы снизить тариф конкретному водителю, но не вправе это сделать. Теперь это становится возможным.

И все-таки. Вырастет ли цена полиса в среднем?

Авторы реформы уверяют, что в среднем стоимость полиса может возрасти незначительно, а для добросовестных, аккуратных водителей даже снизится. Лихачам же и хроническим нарушителям ПДД придется раскошелиться.

«Мы предлагаем изменить систему, чтобы каждый платил сам за себя, а у страховых компаний была возможность использовать дополнительные критерии для оценки водителей. Тогда они смогут предлагать более дешевые полисы для аккуратных водителей, и устанавливать справедливую стоимость для лихачей. Сейчас это невозможно, даже для таких горе-водителей, как житель Сочи, который, заплатив за полис ОСАГО всего 2300 рублей, за 3 месяца попал в 5 аварий с суммарным ущербом в 2,2 миллиона рублей», - говорит Филипп Габуния.

Будут сохранены ограничения и на максимальную стоимость полиса. В том случае, если страховщик попытается завысить тариф, надзорный орган в лице ЦБ потребует привести стоимость полиса в соответствие.

«Лояльность клиентов страховой компании – залог сбалансированности ее портфеля, она открывает возможность для успешного предложения им других страховых продуктов и услуг, говорит представитель одной из страховых компаний. -С учетом высокой конкуренции за таких клиентов странно ожидать, что кто-то из страховщиков будет отпугивать их повышением тарифов, – говорит он. – Напротив, мы ожидаем, что расширение тарифного коридора позволит для части автомобилистов стоимость полиса снизить, а не поднять. И тогда действительно справедливой она будет как для более аварийных и рисковых страхователей, так и для аккуратных и безубыточных водителей.»

И еще одна немаловажная деталь. Рассчитать предварительную стоимость полиса при таком детализированно-индивидуальном подходе самостоятельно практически невозможно. Но выход из положения найден. Страховые компании будут обязаны разместить на своих интернет ресурсах специальные автоматические калькуляторы. Занес требуемые данные – получил стоимость полиса.

И как говорится на закуску, снижение тарифа на 7% прогнозируется в Санкт-Петербурге и Ленинградской, а также в Тверской и Костромской областях для водителей в возрасте от 35 лет, имеющих стаж от 5 лет, КБМ класса 5 и выше и транспортное средство мощностью от 100 лошадиных сил. На 14% может снизиться стоимость полиса для жителей

Пермской, Тюменской, Вологодской, Тульской, Тамбовской и Калининградской областей, а также республик Коми и Удмуртия (автовладельцы транспортных средств мощностью 100 л.с. и более в возрасте от 55 лет, со стажем от 5 лет с КБМ от 5 класса)».

- **RT – Страховые компании могут обязать фиксировать продажу полисов ОСАГО на видео**
  https://russian.rt.com/russia/news/557815-strahovye-kompanii-video-osago

«На страховые компании могут возложить обязанность вести видеозапись продажи полисов ОСАГО.

Об этом «Известиям» рассказал председатель комитета Госдумы по финансовому рынку Анатолий Аксаков.

По его словам, соответствующие поправки уже готовят в закон об ОСАГО, их внесут в парламент в осеннюю сессию.

«Затраты страховщиков будут минимальными, мы знаем, что эта аппаратура стоит копейки. ОСАГО в рамках принятия поправок не подорожает. Мы будем за этим следить. Аудио- и видеозаписи будут храниться в течение всего срока действия договора в специально созданной единой базе данных», – сказал он.

Предполагается, что данная мера позволит снизить число отказов в продаже полисов и избежать навязывания дополнительных услуг клиентам.

При этом эксперты заявили изданию, что принятие поправок всё же внесёт коррективы в стоимость страховки, что приведёт к тому, что полисы могут подорожать на 5%.

Ранее в Госдуму был внесён законопроект, предусматривающий исполнение страховщиками обязанностей по возмещению ущерба и судебных расходов в результате ДТП».

8. Кейс «Криптопирамидное»

Для работы над этим кейсом обратите внимание на материалы Банка России, формулирующие основные признаки финансовой пирамиды. Материал о «финансовых пирамидах» размещен в разделе «Вопросы и ответы» Интернет-приёмной Банка России по адресу: https://www.cbr.ru/reception/faq/finp/. На сайте предоставлены ответы на следующие вопросы:

- По каким признакам можно распознать «финансовую пирамиду»?
- На что должны обратить внимание граждане, чтобы не попасться на «удочку» мошенников?
- -Какие меры для пресечения деятельности «финансовых пирамид» принимает Банк России?

Иные полезные материалы расположены на сайте Fincult.info (информационно-просветительский ресурс Банка России) по ссылке https://fincult.info/article/finansovaya-piramida-kak-ee-raspoznat/.

Кроме того, материал о признаках финансовой пирамиды размещен в разделе «Финансовые рынки» на странице "»Защита прав потребителей финансовых услуг и инвесторов» («Обращения потребителей финансовых услуг и инвесторов») по адресу http://www.cbr.ru/finmarket/protection/protection_treatment/#highlight=%D1%84%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D0%BE%D0%B2%D1%8B%D1%85%7C%D1%84%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D0%BE%D0%B2%D0%B0%D1%8F%7C%D0%BF%D0%B8%D1%80%D0%B0%D0%BC%D0%B8%D0%B4%D0%B0%7C%D1%84%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D0%BE%D0%B2%D0%BE%D0%B9%7C%D0%BF%D0%B8%D1%80%D0%B0%D0%BC%D0%B8%D0%B4%D0%BE%D0%B9%7C%D0%BF%D0%B8%D1%80%D0%B0%D0%BC%D0%B8%D0%B4%D1%8B.

- **В связи с обилием разнообразной информации по указанному адресу, приводим опубликованные ответы Банка России на вопросы о финансовых пирамидах полностью:**

«Что такое финансовая пирамида? Есть ли определение понятия «финансовая пирамида» в российском законодательстве?

В настоящее время в российском законодательстве такое определение отсутствует.

Но чаще всего под финансовой пирамидой понимается мошенничество, незаконное предпринимательство, незаконная банковская деятельность, а также другие преступления, связанные с хищением денежных средств у населения путем обещания имущественной выгоды, получаемой:

- исключительно за счет привлечения денежных средств от иных лиц;
- от инвестиций в финансовые или материальные активы либо проекты, заведомо неспособные обеспечить такую выгоду;
- от инвестиций в финансовые или материальные активы либо проекты без намерения их осуществления.
- Банк России выделяет несколько внешних признаков, по которым можно определить финансовую пирамиду, и выделяет пять основных видов пирамид.

Какие основные признаки финансовой пирамиды?

- Организации, физические лица или публичные проекты, являющиеся финансовой пирамидой, чаще всего обладают одним или сразу несколькими внешними признаками, такими как:
- массированная реклама в СМИ, Интернете, в том числе социальных сетях, с обещанием высокой доходности, значительно превышающей рыночный уровень;
- организация бизнеса на принципах сетевого маркетинга, когда доход участника (инвестора/вкладчика) формируется за счет инвестиций/вложений новых, привлекаемых им участников;
- отсутствие точного определения деятельности организации, физического лица или публичного проекта (заявление об уникальной деятельности);
- наличие предварительных (специальных) взносов для последующего участия в деятельности организации или проекта;
- гарантирование доходности (запрещено на рынке ценных бумаг);
- использование в наименовании, символике, рекламных объявлениях слов и словосочетаний или символики, делающих их похожими на известные компании, бренды (банки, микрофинансовые организации);
- неспособность подтвердить направление размещения привлеченных средств и информацию об этом. - привлечение средств населения в различного рода программы, в том числе на приобретение автомобилей, квартир, земельных участков, товаров народного потребления и т.п., выступающие в качестве альтернативы банковскому кредиту;
- регистрация организации в офшорной юрисдикции (Кипр, Сингапур, Сейшельские острова и т.п.), если финансовая пирамида организована в форме юридического лица;
- отсутствие публичного офиса или наличие исключительно номинального офиса, например по месту регистрации юридического лица или по месту проживания физического лица;
- организация (финансовая пирамида) зарегистрирована за несколько месяцев до начала активной деятельности по привлечению средств, имеет минимальный уставный капитал, единственного учредителя и руководителя или учредителя и руководителя, являющего массовым (подставным) учредителем юридических лиц, например по данным ЕГРЮЛ ФНС России или базы данных СПАРК Интерфакс;
- отсутствие лицензии ФКЦБ/ФСФР России или Банка России на осуществление деятельности по привлечению денежных средств или иной лицензии;
- Особенности предлагаемого к заключению договора:
- основанием для привлечения денежных средств от населения выступает уникальный договор, не имеющий широкого распространения в финансово-хозяйственной практике, например договор финансирования или договор целевого финансирования;
- договор сформулирован таким образом, что у организации, физического лица или публичного проекта отсутствуют какие-либо обязательства перед инвестором (вкладчиком) денежных средств;
- договор сформулирован таким образом, что возврат инвестором (вкладчиком) денежных средств становится невозможным даже в случае прекращения договорных

отношений и невыполнения обязательств со стороны организации, физического лица или публичного проекта.

Информация в сети Интернет на сайте организации:

- сайт организации некачественный (дешевый), часто размещенный на бесплатных (дешевых) хостинговых центрах;
- сайт организации зарегистрирован в офшорной юрисдикции и при этом содержит информацию только на русском языке;
- отсутствие на сайте учредительных документов, если финансовая пирамида организована в форме юридического лица;
- отсутствие на сайте какой-либо информации о финансовом положении организации (отчетов, балансов и т.п.);
- анонимность – отсутствие на сайте конкретной информации об учредителях и руководителях организации или проекта (фамилия, имя, отчество, биография);
- отсутствие информации о собственных основных средствах, других дорогостоящих активах.

При оценке организации, физического лица или публичного проекта следует учитывать, что наличие вышеуказанных признаков лишь косвенно свидетельствует о том, что это финансовая пирамида (каждая финансовая пирамида обладает одним или несколькими указанными признаками, но не каждая организация, физическое лицо или публичный проект с указанными признаками является финансовой пирамидой).

Куда могут обратиться пострадавшие от деятельности финансовой пирамиды, чтобы вернуть вложенные (инвестированные) денежные средства?

Прежде всего, пострадавшим от деятельности финансовой пирамиды необходимо обратиться в правоохранительные органы.

Для возможной компенсации похищенных денежных средств рекомендуем также обратиться в Федеральный общественно-государственный фонд по защите прав вкладчиков и акционеров (105187, Москва, Измайловское шоссе, д. 71, стр. 8; тел: (495) 741-00-74, 989-72-80).

Куда можно обратиться, если в деятельности организаций или физических лиц выявлены внешние признаки финансовой пирамиды?

Если вы выявили признаки финансовой пирамиды в деятельности какого-либо юридического или физического лица, можете направить информацию об этом в правоохранительные органы в любое территориальное учреждение Банка России по месту регистрации (деятельности) предполагаемой финансовой пирамиды, либо в интернет-приемную Банка России.

Полезные сведения содержатся на информационно-просветительском сайте Банка России Fincult.info в материале «Финансовая пирамида: как ее распознать» по адресу: https://fincult.info/article/finansovaya-piramida-kak-ee-raspoznat/».

8.1. Материалы о финансовых пирамидах на рынке криптовалют

8.1.1. Обзорные и экспертные материалы, а также мнения и рекомендации участников рынка

В представленных обзорных материалах рассматриваются основные признаки и характеристики криптовалютных пирамид, обсуждаются проблемы их идентификации, даются авторские рекомендации для инвесторов и для регулирующих органов.

- **Журнал ForkLog – Криптовалютные пирамиды – как не стать жертвой онлайн-мошенников**
  https://forklog.com/cryptoscams-alert/

«Биткоин часто называют инструментом финансовой свободы, который делает ненужными правительства, банки и других посредников, а также предлагает возможность осуществления быстрых и недорогих денежных переводов в любую точку мира.

Однако ряд свойств биткоина, и в первую очередь это касается псевдонимности транзакций, вызывают беспокойство регуляторов, ведущих борьбу с финансированием терроризма и незаконным отмыванием денег.

Большинство усилий регуляторов при этом направлено на приведение в соответствие с законодательством деятельности бирж, предлагающих обмен биткоина и других цифровых валют в фиат. Однако существует одна область, по-прежнему остающаяся для регуляторов «серой зоной»: стремительно набирающий популярность рынок так называемых «инвестиционных программ» с использованием криптовалют.

Часто подобные программы являются ничем иным, как банальными финансовыми пирамидами (также известными как схема Понци). Они обещают необычно высокую доходность (часто выше 30% – 40% в месяц) с минимальным, как утверждается, риском для инвесторов.

Однако в действительности такие схемы генерируют прибыль для ранних инвесторов за счет притока «свежих» средств от новых участников. Пока не прекратится поток новых инвесторов, программа будет выплачивать дивиденды более ранним, после чего обычно закрывается. Либо же организаторы пирамиды попросту решают, что собрали достаточно денег, и исчезают.

Идея аферы далеко не нова и была впервые использована еще в 1919 году клерком из Бостона Чарльзом Понци, но с появлением криптовалют она определенно получила свежее дыхание.

Новые возможности

Традиционно для запуска схемы Понци ее организатору требуется наличие юридического лица (как правило, в виде компании с ограниченной ответственностью) и банковский счет, на который поступают депозиты инвесторов. Поскольку в большинстве стран действуют строгие требования относительно выдачи лицензий на прием депозитов и рекламу инвестиционных продуктов, схемы Понци часто маскируются.

Организаторы могут использовать некий физический продукт, например, биодобавки или ваучеры пополнения телефонных счетов, или же, легитимируя бизнес, предлагают «образовательные программы». Также нередко используется принцип сетевого или многоуровневого маркетинга (MLM) – системы розничных продаж, в рамках которой каждый участник одновременно проводит рекламу и продажу товара потенциальному покупателю.

С появлением биткоина многие препоны юридического характера организаторам схем удается успешно обходить – ни открытия компании, ни банковского счета для осуществления транзакций не требуется, а продукты зачастую представлены в цифровой форме.

Сегодня организаторы криптовалютных пирамид играют на том, что, хотя биткоин и начинает становиться все более известным на мейнстрим-уровне, его понимание среди некоторой части пользователей является максимально упрощенным. Зачастую оно ограничивается ассоциациями с примерами людей, ставшими за одну ночь миллионерами, использованием в качестве платежного средства в даркнете или громкой историей с коллапсом Mt Gox.

Именно обещание быстрого обогащения и делает подобные схемы столь привлекательными для неискушенных пользователей, которые видят в биткоине еще один сияющий объект, часто упуская из вида его истинную природу.

Виды криптовалютных пирамид

Можно выделить три наиболее распространенных вида финансовых пирамид с использованием криптовалют:

- Облачный майнинг;
- Высокодоходные инвестиционные программы;
- Scamcoins – альткоины с «гарантированным» повышением стоимости капитала.

Рассмотрим каждый из этих видов более подробно.

Облачный майнинг

Выдающие себя за облачный майнинг программы плодятся в сети едва ли не каждый день, предлагая приобрести хэшевую мощность или аренду оборудования для майнинга. Взамен пользователям обещают исключительно высокие доходы: по заверениям организаторов, возврат инвестиций и выход в плюс возможен уже через несколько месяцев или даже недель.

Встречая в сети подобные предложения, следует помнить, что в сегодняшних реалиях майнинг – далеко не такое прибыльное занятие, которым он был еще несколько лет назад. Возросшая сложность биткоина в комбинации с состоявшимся летом 2016 года халвингом и другими факторами делают его целесообразным разве что в промышленных масштабах, при этом проверенные и известные компании, если и предлагают облачный майнинг, предпочитают заключать долгосрочные контракты. Ни о каких сверхвысоких доходах при этом речь сегодня даже не ведется, к тому же вряд ли можно увидеть и некую фиксированную процентную ставку на инвестиции.

Отдельные операторы мошеннических сайтов, предусмотрев и этот фактор, в попытке привлечь средства пользователей утверждают, что занимаются майнингом сразу нескольких криптовалют. Верифицировать правдивость таких заявлений становится еще сложнее, но обычная логика подсказывает, что если бы такая деятельность действительно была бы настолько прибыльной, операторам было бы выгодней заниматься этим самим, не предлагая никаких виртуальных контрактов.

Инвестиционные программы

Операторы другого популярного вида криптовалютных пирамид утверждают, что являются опытными трейдерами (и иногда даже якобы используют торговых ботов) или вовлечены в сделки по арбитражу. Точно так же они обещают высокую доходность, часто в районе 3-5% в день. Длительность базового плана часто составляет 28 дней, что и можно считать условным временем жизни подобной пирамиды: второй или третий цикл подобные сайты завершают крайне редко.

Известно, что даже самые лучшие и опытные трейдеры не могут постоянно совершать прибыльные сделки, а такого понятия, как беспроигрышная торговая стратегия, попросту не существует. Успешный криптовалютный трейдинг – это не только умение своевременно идентифицировать возможности и периоды волатильности, делая предположение о вероятном движении рынка. Это еще и умение управлять рисками и потерями, получая прибыль поэтапно и устанавливая правильные стоп-лоссы. Более того, успешным трейдерам, даже если они и переживают неизбежные периоды неудач, в действительности нет необходимости использовать средства других людей, если только они не оказывают профессиональные услуги.

Scamcoins

Вряд ли будет преувеличением сказать, что многие пользователи начинают интересоваться биткоином в надежде на быстрое обогащение, но все они вскоре понимают, что этот поезд ушел. Именно тут и вступает в дело сравнительно новый вид мошеннической схемы: фейковые альткоины, заявленные в качестве улучшенной версии биткоина или криптовалюты, полный потенциал которой еще только предстоит реализовать.

Как правило, упор делается на то что именно сейчас, когда монета мало известна и сравнительно недорого стоит, ее и нужно приобретать, после чего счастливому обладателю такого актива попросту остается дождаться вожделенного туземуна.

Часто такие схемы сопровождаются даже неким подобием whitepaper, призванным ввести в заблуждение тех, кто не очень хорошо разбирается в криптовалютах, или дорожной картой, основной акцент в которой делается на то, как со временем монета будет расти в стоимости.

Более искушенные организаторы даже прибегают к услугам специализированных криптовалютных изданий, на платной основе размещая пресс-релизы, призванные легитимировать их деятельность в глазах сообщества. Нередко подобные проекты не имеют ни публичных блокчейнов, ни находящегося в открытом доступе кода, а весь «трейдинг» осуществляется в рамках самой платформы или определенной сети сайтов, являясь по сути ничем иным, как обычной манипуляцией, призванной создать видимость некой активности и постоянно растущей цены.

Как распознать криптовалютные пирамиды

Идентифицировать мошеннические схемы с использованием криптовалют для рядового пользователя часто бывает непростой задачей. Попасться в сети мошенников могут при этом и те, кто имеет какое-то представление о криптовалютах – организаторы схем с каждым днем становятся все более изощренными, не жалея ни средств, ни времени на создание очередного привлекательного и яркого внешне, но являющегося пустышкой внутри сайта.

Тем не менее, определенные общие признаки, говорящие о том, что перед вами пирамида, безусловно, существуют.

Обещание стабильных высоких доходов. Если это звучит слишком хорошо, чтобы быть правдой, то, скорее всего, правдой это и не является. При этом, чем выше обещанный доход, тем выше оказываются риски. Также следует помнить, что все без исключения пирамиды начинают с того, что поначалу действительно выплачивают обещанные средства, поскольку иначе новых пользователей им попросту не завлечь. Все это, однако, длится ровно до того момента, пока организаторы не решат, что свою задачу-минимум выполнили. После этого они исчезают вместе с деньгами вкладчиков.

Необходимость привлекать рефералов. Если заработок предполагает необходимость иметь рефералов (т.е. новых участников, регистрирующихся по вашей личной ссылке) – это очевидный тревожный сигнал, говорящий о том, что вы имеете дело с моделью, которая не приносит настоящей прибыли.

Отсутствие информации о владельцах. Еще один «красный флаг» – отсутствие данных о владельцах ресурса. Честные и легитимные проекты такую информацию не скрывают, и быстрый поиск в сети может выдать историю о человеке, если он действительно существует.

Необходимость регистрации для получения дополнительной информации о проекте. Часто в сети можно натолкнуться на яркую и украшенную завлекающими фразами рекламу проектов по заработку в сети, однако подробную информацию о том, как «уволить своего босса», можно получить лишь после регистрации с указанием имени и адреса электронной почты. Нередко «содержимое» сайта сильно отличается от того, на что «клюнул» пользователь.

Закрытый код, закрытый блокчейн. Практически во всех случаях с упомянутыми выше Scamcoins вы не встретите ни открытого кода, ни публичного блокчейна, что для подавляющего большинства криптовалют считается элементарным знаком хорошего тона. Некоторые наиболее продвинутые проекты, впрочем, могут предлагать симуляторы блокчейна на своих сайтах, а иногда даже оказываются включенными в список альткоинов на Coinmarketcap.com.

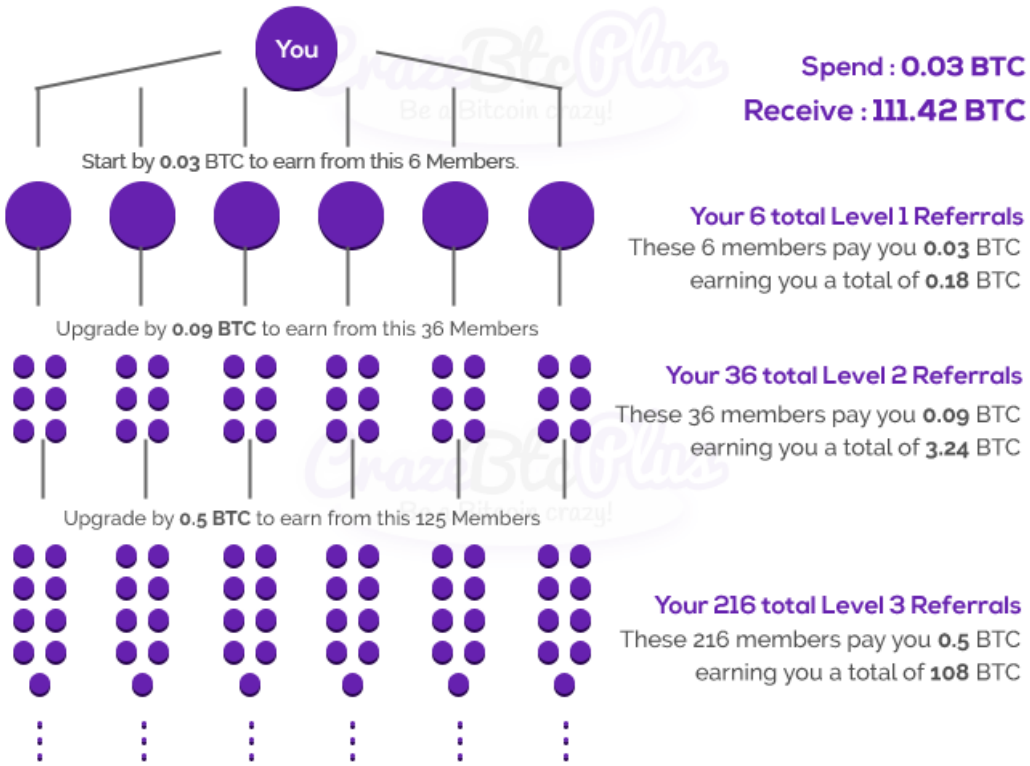
Отсутствие монеты на заслуживающих доверия биржах. Легитимность проекта можно проверить, узнав, торгуется ли заявленная монета на какой-либо из известных бирж с доступным API. Справедливости ради следует отметить, что иногда добавление криптовалют на биржи может занять некоторое время. Помимо этого, крайне важно, чтобы проект имел ссылку на публичный URL с указанием общего объема доступных монет. Если проект предлагает обмен только в рамках своей платформы, будет разумным решением держаться от него подальше.

Дополнительно проверку сайта можно провести на badbitcoin.org – данный ресурс содержит регулярно обновляемый список большинства известных скам-проектов.

Условное мошенничество

Отдельно следует упомянуть еще один набирающий популярность вид онлайн-программ, использующих биткоин. Известные как «матрица», такие программы

предполагают p2p-платежи между участниками, обещая потенциальный заработок в десятки или даже сотни биткоинов в месяц.



Классическая схема «матрицы» с многоуровневой реферальной системой

Есть, здесь, правда, один немаловажный нюанс: сама схема, возможно, и является рабочей, однако требует от пользователя умения привлекать новых пользователей, поскольку именно за счет рефералов и строится заработок.

В то же время создание аффилированных структур – это отдельная наука, и расставаться с кровно заработанными монетами, если вы не уверены в своих возможностях в области онлайн-маркетинга, было бы слишком необдуманно. В противном случае вас, скорее всего, ждет сценарий, при котором вы отправите другому пользователю условные 0.01 BTC, но на этом все для вас и закончится: найти желающих сделать аналогичный перевод вам будет очень непросто.

В заключении хочется подчеркнуть одну главную мысль: спрос рождает предложение, и не питай многие пользователи сети часто тщетных надежд на быстрый заработок, подобных схем было бы на порядок меньше. Будьте ответственны в своих решениях».

- **Блокчейн и криптовалюты в России – Криптовалютные пирамиды. Чем отличаются и как определить?**
  https://cryptorussia.ru/zametki/kriptovalyutnye-piramidy-chem-otlichayutsya-i-kak-opredelit

«Скандал с Кэшбери породил очередную волну опасений, так как пирамиду поспешили признать «криптовалютной». Есть ли разница между этой и другими финансовыми пирамидами и как обезопасить себя от мошенников? Об этом Cryptorussia рассказали эксперты.

Криптовалютная или финансовая пирамида?

Эксперты сходятся во мнении, что у так называемой криптовалютной пирамиды не так много отличительных особенностей от обычных финансовых пирамид. Они обладают теми же качествами, но с прибавкой, например, о возможности инвестирования цифровых активов. В другом случае это, например, проект с привлечением средств по принципу ICO.

Главным отличием криптовалютной пирамиды от финансовой эксперты называют правовые нюансы. Из-за отсутствия регулирования криптовалютного сектора в России фактически основатели криптовалютных пирамид не могут предоставить каких-либо документов и дать какие-либо гарантии. Со стороны инвестора нет возможности защитить собственные вложения.

«Криптовалютная компания не может предъявить вообще ничего, – объясняет президент инвестиционного дома RPK Capital Михаил Поликутин. – На сегодняшний день криптовалюта не является платежным средством в РФ, не регулируется законом и т.д. Поэтому криптовалютная пирамида не может предъявить никаких документов. Если в обычной финансовой пирамиде вы можете подписать какие-то бумаги, получить документальное подтверждение об обязательствах о возмещении средств и, хотя бы в теории, потом предъявить претензии, в случае с криптовалютой ничего подобного не будет. В текущем правовом поле вы будете полностью бесправны»

Менеджер по развитию торговой инфраструктуры компании Zichain Данил Яковлев вспоминает, что в конце прошлого года многие инвесторы легко теряли бдительность при упоминании слов «блокчейн», «децентрализация» и «токенизация»:

«Ситуация не сильно улучшилась в этом году. Мошенники пользуются преимуществами криптовалют, за счет которых можно собрать деньги с инвесторов, не пересекаясь с государством и финансовыми регуляторами»

Принципиальных отличий классических способов инвестирования от тех, что связаны с криптовалютой – нет, считает руководитель проектов ICO «Прифинанс» Николай Тимофеев. Следовательно, нет отличий и криптовалютных пирамид от обычных.

Что такое финансовая пирамида?

Под пирамидами часто понимаются MLM – способ маркетингового продвижения и продаж. Он применяется много лет. К положительным примерам можно отнести, например, фирму Oriflame.

«Однако, есть нюансы, – объясняет партнер юридической компании GMT Legal Дмитрий Мачихин. – Чертой отличающей "добрый" MLM от грубой мошеннической пирамиды является наличие умысла на обман поздних вкладчиков, а также отсутствие источника пополнения капитала извне. Синоним "злой" пирамиды – схема имени Понци, итальяно-американского мошенника, создавшего аферу, массово давая обещания прибыли вкладчикам за счет вкладов новых участников, образуя пирамиду до момента обвала,

который неизбежно наступает, согласно природе спекуляций и любых финансовых пузырей»

В нашей стране таким мошенничеством отличился Мавроди с пирамидой «МММ».

Дмитрий Мачихин также напоминает, что понятие финансовой пирамиды закреплено на законодательном уровне и за нее можно поплатиться, в том числе лишением свободы до шести лет. Пока практика применения этой уголовной статьи не очень распространена.

«Тем не менее мы нашли несколько обвинительных приговоров, а также нам известно о ряде возбужденных дел», – отмечает Дмитрий Мачихин.

Признаки пирамиды

Центральный банк России дает несколько основных признаков финансовой пирамиды в своих рекомендациях:

- выплата денег участникам из средств, внесенных другими участниками,
- отсутствие лицензий на этот вид деятельности,
- обещание высокой доходности,
- отсутствие информации о финансовом положении организации,
- отсутствие собственных основных средств или активов,
- отсутствие определенного вида деятельности фирмы.

Как отмечает руководитель проектов ICO «Прифинанс» Николай Тимофеев, почти все эти пункты можно соотнести с криптовалютными пирамидами. Исключение – наличие лицензии. Однако этот пункт будет доступен после принятия законов.

Эксперты, опрошенные Cryptorussia, отмечают еще несколько признаков, на которые стоит обратить внимание. Менеджер по развитию торговой инфраструктуры Zichain Данил Яковлев говорит, что мошеннические пирамиды не любят публичности. Настоящие профессионалы не будут рисковать своей репутацией, чтобы вовлечь людей в махинацию. Кроме того, организаторы пирамид могут преувеличивать или вовсе искажать факты.

«В распоряжении мошенников, как правило, не так много информации, которую можно презентовать инвесторам. Соответственно, важная информация о технологии, рынке или бизнес процессах описывается поверхностно, в то время как незначительным фактам уделяется наоборот слишком много внимания», – объясняет Данил Яковлев.

Еще одним пунктом эксперт добавляет агрессивную рекламу проекта.

Президент Инвестиционного дома RPK Capital Михаил Поликутин добавляет в общий список еще один признак – это отсутствие какой-либо документации:

«У пирамид, как правило, нет ничего, кроме сайта, на котором может быть написано все что угодно, но вот получить реальные документы вам вряд ли предложат», – объясняет эксперт.

Руководитель проектов ICO «Прифинанс» Николай Тимофеев в общий список Центрального банка предлагает добавить еще несколько пунктов:

- низкий порог для входа, проекты заинтересованы не в количестве инвесторов,

- еженедельные и ежемесячные выводы прибыли,
- выгодная реферальная программа.

CEO проекта Finside Иван Бабайлов отмечает еще несколько признаков. Он отмечает, что не могут стартапы на этапе ICO гарантировать высокую доходность, так как они могут отвечать только за реализацию проекта. По мнению эксперта, необходимо попробовать поискать информацию о тех, кто просит инвестиций. Это должны быть публичные личности. Также нужно проверять представленную юридическую информацию.

Еще один важный показатель – это присутствие на серьезных биржах, считает Иван Бабайлов.

«Будьте внимательны и инвестируйте только в те проекты, которые создают реальную пользу для мира технологий», – заключает эксперт.

Советы от экспертов

Николай Тимофеев, руководитель проектов ICO компании Прифинанс:

«Ситуация с криптофондами очень похожа на ситуацию с форекс-брокерами. Слабое регулирование, низкая финансовая грамотность населения позволяли мошенникам привлекать огромные средства. Сейчас происходит то же самое, но уже с криптофондами. Более того, большое количество проектов с криптофондами создано теми же людьми, которые недавно работали как псевдо форекс-брокеры.
Если криптофонд соответствует хотя бы двум признаков из тех, которые мы рассмотрели выше, то, скорее всего, это говорит о том, что проект является мошенническим и любые инвестиции в него приведут к потерям средств.
Из-за слабого регулирования вернуть потерянные средства, что-либо взыскать с организаторов проекта будет в большинстве случаев невозможно»

Михаил Поликутин, президент Инвестиционного дома RPK Capital:

«Конечно, нужно начать с того, что просто не верить агитации, которую вы встретите в интернете и советам заинтересованных знакомых, уже состоящих в сетевой структуре. Первым делом надо «пробить» всю информацию о проекте, которую вы сможете найти. Посмотрите, когда был создан тот или иной сайт, когда был зарегистрирован домен. Если компания заявляет, что она надежна, а создана неделю назад, вывод делайте сами. Поищите комментарии в интернете: если пирамида существует хотя бы несколько месяцев, наверняка ее уже где-то обсуждали. Если в интернете ничего нет, то это может быть либо ранняя стадия истории, либо, например, пирамида, зашифрованная под ICO. То есть кто-то собирает деньги под продукт, который никогда не будет выпущен. Чтобы понять, возможно ли запустить продукт подобного характера, необходимо посмотреть, есть ли на рынке что-то подобное. Если нет, а их чаще всего это именно так, стоит обратиться к экспертам и получить консультацию, прежде чем отдавать реальные деньги. На сегодняшний день сбор средств с помощью ICO достаточно распространен. Но доверие к ним уже не то. Посмотрите, кто в этих ICO является консультантами, обязательно проверьте их истории «на чистоту», сделать это можно с помощью элементарного поиска в интернете. Если за проектом нет серьезных игроков, банков, страховых и других компаний, которые дорожат своим именем, которые участвуют в том числе в инвестировании в эти ICO на ранней стадии, заходить в такие проекты я не рекомендую»

Лилия Алеева, Директор по маркетингу ICL Services, кандидат экономических наук:

«Первый и главный признак любой пирамиды – это сверхдоходность, разительно сильно превышающая среднюю доходность по соответствующему рынку. На финансовом рынке это могут быть одни показатели, а крипте – другие. Объединяет всех всегда одно – вам обещают золотые горы в очень сжатые сроки. Сказка про золотые монеты и Буратино никогда не потеряет своей актуальности. Еще один общий признак – это малое количество доступной об инструменте информации, а решение нужно принять здесь и сейчас, иначе потеряете в доходности. При этом информации не хватает ни о владельцах проекта, нет находящегося в открытом доступе кода, да и с другими признанными площадками проект не интегрирован, профессиональным сообществом проект не признан. Стимуляция принятия решения быстро, в спешке при нехватке информации снижает вашу защищенность от мошенничества, и этим инструментов всегда пользуются мошенники. Еще один тревожный звоночек - что для поддержания своего дохода или его прироста вам обязательно нужно привлекать еще людей. Любая пирамида держится на объеме привлеченных участников, когда доход от последующих выплачивается предыдущим участникам. Стимуляция этого роста как обязательное условие сразу должно вас насторожить.»

Дмитрий Мачихин, партнер юридической компании GMT Legal:

«Прежде всего стоит опасаться космических предложений доходности и агрессивной рекламы. Если о пирамиде N знают все, значит вы уже будете не в основании. Следует обязательно проверить компанию и провести due dilligence (юридический аудит). Вся информация должна быть открыта, у создателей должна быть кристальная репутация. И конечно стоит внимательно читать договор и изучать риски. Пирамида, созданная исключительно с целью сбора максимального количества средств, особенно когда эти средства зафиксированы в криптовалютах, наделенных дикой волатильностью, обречена на крах в любом случае. Помните это, выбирая способы инвестирования».

- **Mining-Bitcoin – Можете ли вы распознать пирамиду криптовалют?**
  https://mining-bitcoin.ru/news/kriptovalyuta-piramida

1. «Инвесторы криптовалюты про финансовые пирамиды
2. Как проверить сервис по работе с криптовалютой
3. Признаки пирамид криптовалюты

Пока цены на биткоин падают, приверженцы цифровых валют пытаются выяснить причины кризиса. Помимо опасений из-за действий регуляторов, потенциальных инвесторов отпугивает тот факт, что слова криптовалюта пирамида слишком часто появляются в новостях, посвящённых мошенническим операциям.

В январе 2018 основателей сайта Bitconnect обвинили в раскрутке преступной схемы. Тени подозрения оказалось достаточно, чтобы мгновенно обрушить цену валюты сайта на 90%. Инвесторы, анализирующие преимущества облачного майнинга криптовалюты и ICO-платформ, также сталкиваются с проблемой верификации и проверки надёжности сервисов.

Как выявить создателей пирамиды криптовалют, если даже опытные участника рынка порой попадают впросак? Мы собрали несколько способов, которые пригодились для развенчания недавних крупных схем.

1. Инвесторы криптовалюты про финансовые пирамиды

Среди специалистов существуют разногласия по поводу валидности цифровых активов. Трейдер Престон Баннистер убеждён, что биткоин, как и всякая другая криптовалюта, по самой своей природе похож на пирамиду.

У BTC нет привязки к стоимости, поэтому если его не используют как платёжное средство в государстве со стабильным правительством, у него нет будущего.

Так ли это? Эксперты проводят параллели между криптовалютой и игорным бизнесом – пока кто-то готов платить за токены, их цена будет расти. Но организатор биткоин-конференции Эллери Дейвис предлагает сравнивать Bitcoin не с пирамидой, а с живописью Пикассо. Отвечая на вопрос о надёжности криптовалюты по сравнению со слитками драгоценных металлов, он отмечает:

В отличие от золота, Bitcoin – чисто математический концепт. Но точно так же, как и в случае с золотом и живописью Пикассо, его стоимость определяется спросом и предложением. Это не имеет ничего общего с пирамидой.

2. Как проверить сервис по работе с криптовалютой

Традиционные инвесторы советуют не доверять компаниям, которые обещают более 20% годовой прибыли, но этот совет едва ли применим для криптовалют. В мире блокчейна речь идёт о сверхприбылях. Главная проблема – убедиться, что вы имеете дело с реальными людьми, а не изобретателями пирамиды. Если появилась новая платформа, выполните несколько действий:

1. Проверьте страницу «О нас» в описании компании. Есть ли на ней информация о создателях и адрес регистрации? Отыщите фотографии в поиске изображений Google. В пирамиде криптовалют Benebit они были украдены.
2. Используйте сайты анализа доменов для проверки данных (GoDaddy). «Приватная регистрация» может означать, что вы имеете дело с пирамидой.
3. Возраст домена. Убедитесь, что сайту как минимум 6 месяцев. Лучше больше. Если рейтинг Alexa на уровне 200 тыс. и меньше, такие сайты о криптовалюте считаются более надёжными.
4. Обращайте внимание на метрики авторитетности домена и качество ссылок, ведущих на сайт (сервис MOZ). DA должна быть выше 20.
5. Изучите отзывы в Google и на форумах (Bitcointalk, Reddit). Помните, что отрицательные могут быть написаны конкурентами, а положительные – организаторами пирамиды.

3. Признаки пирамид криптовалюты

К концу 2017 года в новостях стала все чаще мелькать информация о фальшивых ICO. Многие попались на типичной ошибке создателей пирамид криптовалют – недостоверности публичной информации. Centra Tech и Benebit использовали фальшивые фотографии участников команды.

Мари Ясек из Университета Нью-Мексико и Тайлор Мур из Университета Талсы (Оклахома) утверждают:

Мошеннические схемы появляются практически ежедневно.

На сайте Entrepeneurs Headquarters писали, что компания базируется в Великобритании, тогда как CEO этой пирамиды был молодой человек, живущий в Колорадо. По лондонскому адресу журналисты нашли только разрушенный дом. А также отсутствовал контактный номер телефона».

- **CryptoWikipedia – КРИПТОВАЛЮТА ЭТО ПИРАМИДА?**
  https://cryptowikipedia.ru/kriptovalyuta-yeto-piramida/

«Несмотря на разрастающуюся популярность цифровых денег, отзывы о них и сегодня встречаются самые разные, в том числе и негативные. Наиболее распространенными являются отклики на тему: криптовалюта это пирамида и когда она рухнет, когда случится очередной глобальный экономический кризис. Правда, эксперты по большей части опровергают такой апокалиптический сценарий развития событий. А панику создают в основном те, кто не совсем четко представляет себе принцип функционирования криптовалюты. Хотя справедливости ради стоит отметить наличие общих черт у некоторых криптовалютных проектов и финансовых пирамид, но речь идет о частных случаях, а не никак не об общей тенденции. Отличий между виртуальными активами и очередным аналогом МММ гораздо больше.

Криптовалюта это пирамида или нет

Рядовому пользователю немудрено запутаться в вопросе: криптовалюта это финансовая пирамида или нет? Когда со всех сторон звучат высказывания о том, что цифровые деньги – крупнейшая афера нового века, поверить в это легко. Но если подходить к теме с критической точки зрения, то сразу становится понятно, что истина наскоро сметана белыми нитками. Финансовые пирамиды – это, по сути, **мыльные пузыри**, которые закономерно лопаются, когда чересчур раздуваются.

Структура такого проекта выглядит предельно просто: на верхушке стоит один человек, который привлекает еще нескольких участников разных уровней, они платят за подключение к системе, с этой суммы отдаются дивиденды тем, кто находится на более высоких ступенях.

Принцип работы криптовалютных систем

Криптовалютные системы работают по другому принципу. С финансовыми пирамидами их сравнивают из-за наличия этапов предпродаж и ICO, когда на еще не созданный проект собираются фиатные деньги, которые потом меняются на токены. Однако в данном случае никаких ступней и уровней не образуется. Да и вкладчики отдают свои средства не для непонятной цели, а для финансирования обоснованного проекта на платформе блокчейна, более подробная информация в статье «Принцип криптовалюты»

- Уж существование этой технологии точно невозможно подвергнуть сомнению, несмотря на то, что существует она только в виртуальном пространстве.
- Но при этом вполне успешно используется в самых разных сферах реальной жизни, начиная от денежных переводов и заканчивая соцсетями.

- А криптовалюта – это еще одно проявление блокчейна: цифровые деньги с абсолютным уровнем защиты и высокой степенью анонимности.

Эти монеты, снабженные криптографическими кодами, генерируются с помощью майнинга при проведении транзакций либо выпускаются всей массой в момент ICO. Наличие таких виртуальных активов открывает для разных блокчейн-платформ новые возможности для расширения, развития и привлечения участников. Но разрастаются такие системы не вширь, как пирамиды, а скорее напоминают ветвящиеся кроны деревьев.

Отзывы экспертов о криптовалюте

Отвечая на вопрос: «Криптовалюта это пирамида или будущее?» эксперты приводят массу отличий между двумя явлениями современного финансового рынка. Во-первых, цифровые деньги не зря получили свое название. Это не пресловутые акции МММ, которые по сути были бумажками. Токены служат для оплаты услуг внутри системы и товаров в интернет-магазинах, их можно продавать и покупать на бирже или откладывать «на черный день». Во-вторых, обзор рынка криптовалют позволяет судить, что большинство из них базируются на успешно работающих, востребованных платформах, которые имеют практическую ценность. А раз этими системами активно пользуются, то и токены находятся в обороте и следовательно растут в цене – приносят реальную прибыль. В-третьих, у блокчейна нет центра – пирамиду же контролирует один человек. В-четвертых, некоторые криптовалюты прекрасно могут существовать без генерации новых монет – ограниченная эмиссия не мешает привлечению новых членов, потому что для них всегда есть особый резерв токенов. В-пятых, цифровые деньги в некоторых странах получили официальный статус и были включены в национальную экономическую систему – их владельцы и майнеры платят налоги как за деятельность, приносящую финансовый доход».

- **РБК – ЦБ предупредил о маскировке финансовых пирамид под ICO** **https://www.rbc.ru/finances/04/04/2018/5ac4cc0d9a79472c65f1b3b9**

«По словам главы департамента ЦБ Валерия Ляха, мошенничества с первичным размещением токенов являются не чисто российской, но международной проблемой.

О проведении первичного размещения токенов (Initial coin offering, ICO) нередко объявляют мошенники, фактически речь идет о маскировке под ICO новых финансовых пирамид, предупредил директор департамента противодействия недобросовестным практикам Банка России Валерий Лях.

«Сейчас значительная часть финансовых пирамид действительно маскируется под ICO, это проблема в первую очередь не внутрироссийская, это международная проблема, связанная еще и с тем, что фактически идет оказание трансграничных псевдофинансовых услуг», – сказал Лях журналистам (цитата по «РИА Новости»).

Представители Банка России уже не раз высказывали опасения относительно рисков оборота криптовалют, сравнивая их с финансовой пирамидой.

«Очевидно, что во время роста пирамиды интерес к этой пирамиде активно подогревается высокой доходностью», – говорил в октябре 2017 года первый заместитель председателя Банка России Сергей Швецов. «Мы считаем, что для наших граждан использование таких криптовалют в качестве объектов для инвестирования несет неоправданно повышенный риск», – добавлял он.

Советник международного секретаря IDACB (Международной децентрализованной ассоциации криптовалют и блокчейна) Юлия Хренова полагает, что опасения представителей ЦБ «значительно преувеличены», однако советует инвесторам внимательнее относиться к выбору ICO, в которое они намерены вложиться.

«Проекты ICO, направленные на сбор средств без каких-либо гарантий и выходных продуктов, сильно выделяются на фоне проектов реальных и жизнеспособных. Основными маркерами надежных проектов служат длительность существования до выхода на ICO, пошаговые и подробные дорожные карты с техническими параметрами, наличие прототипа продукта и реальные люди в команде проекта. Особо важна прозрачность компании – владельца токенов. У нее должна иметься информация о регистрации. Кроме того, необходимо обращать внимание на проведение листинга на надежных биржах и сертификацию международных ассоциаций», – пояснила РБК Юлия Хренова.

Низкая грамотность инвесторов

Советник председателя правления ассоциации «Финансовые инновации» Андрей Коркишко заявил РБК, что масштабы махинаций при проведении ICO измеряются сотнями миллионов долларов. «Самый яркий пример из первых крупных ICO – компания Tezos. Она привлекла у инвесторов $230 млн и потом благополучно прекратила существование из-за внутреннего конфликта, сейчас компанию преследуют американские регуляторы и обманутые инвесторы», – отметил он.

По его словам, проблема заключается в низкой финансовой грамотности инвесторов. «Многие люди увидели в криптовалютах элемент быстрого обогащения. Рассказы о сказочном богатстве людей, которые принимали участие в ICO, заставили неопытных инвесторов поверить в это так же, как они верили в МММ или другие финансовые пирамиды. То есть люди думали, что рост биткоинов и других цифровых валют и компаний, которые проводили ICO, никогда не прекратится. Однако этим воспользовались мошенники. Они [мошенники] действовали по простой схеме: они делали красивую обертку, вкладывали значительные средства в пиар и маркетинг, привлекали для рекламы зачастую известные имена», – пояснил Коркишко.

По его словам, чтобы предостеречь себя от ошибок, необходимо тщательно изучать предложения. «Необходимо понимать, во что вы инвестируете деньги, какая будет доходность, не стесняться задавать вопросы людям, которые это ICO проводят, следить за тем, чтобы была прозрачная информация», – добавил он.

По словам директора московского филиала «БКС Премьер» Александра Бахтина, для того, чтобы предостеречь себя от мошенников, частному инвестору необходимо собрать всю доступную информацию о проекте в Сети. «Для начала стоит оценить активность проекта в официальных аккаунтах (к примеру, Twitter, Telegram) и количество их подписчиков, просмотреть состав команды и их профили в LinkedIn, проанализировать white paper. Это позволит отбросить огромное количество сомнительных проектов. Среди проводимых ICO сейчас огромное количество скамовых [мошеннических] проектов. Они благополучно привлекают деньги от частных инвесторов по стандартной схеме и просто исчезают», – пояснил он.

Операционный директор Waves Lab Виталий Цигулев рассказал РБК, на что стоит обращать внимание, чтобы предостеречь себя от ошибок. «Обычно со 100-процентной вероятностью можно сказать, что данный проект – это финансовая пирамида, если вы видите в нем такие признаки, как абстрактные общие лозунги о финансовом благополучии, независимости и успехе, если основная бизнес-идея построена вокруг объединения людей, совместном обучении на онлайн-вебинарах, обещаниях гарантированной доходности, выраженной в фиксированных процентах за месяц», – пояснил он.

По его словам, частных инвесторов должны насторожить упоминания о реферальной сети и возможность получить доступ к особым привилегиям. «[Признаками финансовой пирамиды могут быть присутствующие] в команде никому неизвестные люди с опытом инфобизнеса. Они - талантливые ораторы, но говорят общие популистские вещи о том, как вам будет хорошо, если вы присоединитесь к их проекту», – добавил эксперт.

«Классическая пирамида»

Ведущий аналитик компании Amarkets Артем Деев сравнивал мошенничество в сфере криптовалют со строительством пирамид, к которым у россиян, по мнению аналитика, есть предрасположенность.

«Мошенники рассказывают о том, что такое криптовалюты и биткоины, обещают доходность в несколько сот процентов годовых и собирают у людей деньги. Первым вкладчикам отдаются проценты, тема набирает популярность, а в итоге получается классическая пирамида. И в данном случае не столь важно, каким образом привлекают людей – сервисы облачного майнинга, депозиты или что-либо еще. Смысл пирамиды всегда в высоких процентах и выплатах первым вкладчикам», – говорил Деев.

Сооснователь криптофонда The Token Fund Владимир Смеркис в ноябре 2017 года в разговоре с корреспондентом РБК признал рискованность инвестиций в криптовалюты. В то же время он не согласился с тезисом, что криптовалюты – это та же пирамида.

«Когда мы говорим о криптовалютах, необходимо понимать, что мы говорим не только про спекуляции на курсе. Все-таки за многими проектами, связанными с криптовалютами и ICO, стоят технологии: распределенное хранение данных, приложения для торговли, платежные инструменты», – говорит Смеркис.

Глава группы по предоставлению юридических услуг для технологических проектов компании Deloitte СНГ Артем Толкачев говорил, что на рынке криптовалют царит «массовая истерия», а вокруг ICO надулся финансовый пузырь, который в ближайшее время лопнет.

Однако, по мнению блокчейн-консультанта и представителя блокчейн-платформы Lisk в России Дениса Смирнова, говорить о схлопывании пузыря преждевременно. «Сейчас у эмитентов нет почти никаких юридически регулируемых отношений с инвесторами: с одной стороны, это дает инвесторам возможность получить сверхприбыль, а с другой – оставляет большой простор для мошенничества. Но до тех пор, пока рынок не начнут регулировать, мы увидим еще много успешных ICO», – говорил Смирнов.

Регулирование ICO в России

В конце декабря 2017 года стало известно, что Минфин и Банк России подготовили законопроект о регулировании ICO. В документе в основном оговариваются вопросы

регулирования ICO, так как, по словам замглавы Минфина Алексея Моисеева, именно в этой сфере велика опасность для граждан попасть в руки мошенников.

20 марта проект закона «О цифровых финансовых активах» был внесен в Госдуму. Согласно документу, решение по ограничению суммы приобретения токенов лицами, не являющимися квалифицированными инвесторами, будет приниматься ЦБ «с целью обеспечения защиты неквалифицированных инвесторов».

По подсчетам экспертов исследовательской компании Autonomous, только в первом полугодии 2017 года финтех-стартапы привлекли $1,27 млрд, продавая криптовалюты в рамках ICO. В исследовании отмечалось, что за два года объем средств, привлеченных через ICO, вырос почти в 50 раз (в 2014 году он составлял $26 млн).

Позднее эксперты Ernst & Young, проанализировав данные о 372 ICO, заявили, что примерно $400 млн из $3,7 млрд, которые удалось привлечь организаторам выпуска криптовалют, было похищено».

- **Expert's Blog – Инвестирование в блокчейн-стартапы: биткойн умер, да здравствует биткойн?**
  https://expertprof.com/investirovanie-v-blokcheyn-startapy-bitkoyn-umer-da-zdravstvuet-bitkoyn/

«Блокчейн, криптовалюты, смарт-контракты – всё это неожиданно наступившее технобудущее активно обсуждается последние несколько лет. Так называемый биткойн-бум, внезапно поднявшийся мощнейшей волной в начале 2017 года и так же внезапно сдувшийся к декабрю, затронул интересы подавляющего большинства инвесторов – от мелких спекулянтов и вкладчиков всевозможных криптовалютных проектов (часто банальнейших хайпов) до крупных серьёзных инвестфондов. После резкого падения стоимости абсолютно всех "койнов" многие посчитали, что это было временным помешательством, больше не стоящим внимания – кто-то успел сорвать куш, кто-то потерял все свои вложения, кто-то до сих пор пытается продать на "Авито" ставшие бесполезными дорогостоящие майнинг-фермы.

Однако блокчейн-технологии – это не только майнинг и торговля на бирже абсолютно умозрительными криптовалютами, сложными последовательностями единиц и нулей. Без излишнего пафоса можно сказать, что эта отрасль – настоящее будущее мировой экономики. Похожие скептические настроения в среде инвесторов царили в начале 2000-х годов после краха доткомов, когда акции большинства молодых интернет-компаний, активно росшие в цене несколько лет подряд, резко подешевели в течение считаных недель. Но кто сегодня представляет свою жизнь без интернета, онлайн-платформ, электронных платёжных систем и облачных сервисов, без многомиллиардных интернет-гигантов с их услугами? Стартапы, разрабатывающие на основе блокчейн-цепочек революционно новые методы защищённого, безопасного и быстрого заключения биржевых контрактов и регистрации сделок с имуществом, появляются ежемесячно. Вложившись в проект на ранних этапах, можно успеть вскочить на подножку разгоняющегося поезда прогресса и получить очень неплохой доход – но для этого нужно правильно выбрать перспективный объект вложения. Как это сделать, не нарвавшись на "пустышку" или вовсе мошенническую схему, обсуждаем в сегодняшней статье.

Ликбез

Для начала разберёмся, что же это за зверь такой – блокчейн. Изначально совершенно теоретическое исследование конца 1990-х годов на тему децентрализованных сетей (множества связанных друг с другом узлов без единого управляющего или контролирующего центра) впервые получило практическую реализацию в 2008 году, когда была создана первая криптовалюта – биткойн. Технология основана на выстраивании в одноранговой сети (без единого центра) определённой цепочки логических блоков, в каждом из которых будет содержаться информация обо всех предыдущих действиях с этим блоком – создании, транзакциях – и эти данные будут полностью открыты и доступны любому участнику сети.

В 2013 году была предложена и впоследствии реализована идея смарт-контрактов – “умных” договоров о передаче активов или регистрации права собственности в единой децентрализованной сети. Смарт-контракты могут заключаться между контрагентами и немедленно вступать в силу без лишних бюрократических проволочек. Это открывает возможности для создания, к примеру, рынка ценных бумаг с прямым взаимодействием игроков – не нужны фондовые биржи, трейдинг-центры, брокерские компании, все условия всех сделок с активами будут прозрачны и намертво “зашиты” в цепочках логических блоков, подписанных цифровыми подписями. По тому же принципу, хоть и с участием государственных органов, могут быть созданы реестры права собственности на недвижимость, землю и так далее – вплоть до выдачи полноценных электронных удостоверений личности. Вместо долгих месяцев ожидания проверки документов и мучений с нотариальной регистрацией дом или земельный участок можно будет продать или купить за минуты.

Перспективы вложений в блокчейн-технологии

Стартапы, занимающиеся разработкой и совершенствованием таких технологий, в большинстве своём привлекают инвестиции для продолжения работы через краудфандинговые платформы – также работающие на основе блокчейна. Инвесторы, вкладывая в проект свои деньги (в фиатных валютах, эмитируемых государствами), в обмен получают токены. Если раньше токенами назывались собственно криптовалюты, ничем не обеспеченные сочетания цифр, то сегодня токены, выпущенные в процессе ICO (по аналогии с IPO), являются своеобразными цифровыми акциями стартапа, дающими право на получение в будущем части прибыли этой компании. Общая сумма инвестиций, привлечённых блокчейн-проектами к середине этого года, превысила 6 миллиардов долларов. Крупнейший ICO – выпуск токенов Gram от компании Telegram. Павлу Дурову удалось привлечь 1,7 миллиарда долларов от нескольких десятков крупнейших инвестфондов мира. О вложениях в перспективные разработки в области блокчейн-решений заявляют глава Facebook Марк Цукерберг и сооснователь Google Сергей Брин – это говорит о максимальной серьёзности и перспективности инвестиций в стартапы этой отрасли.

Критерии выбора блокчейн-стартапа для инвестирования

- Подробная техническая информация о проекте. Как ни странно, но оценка экономических перспектив инвестиций в компанию начинается именно с технического анализа документации, поэтому кроме хорошего финансового аналитика вам потребуется привлечь ещё и неплохого программиста с обязательным опытом работы в сфере криптографии и блокчейн-систем. Подробная тщательно расписанная “дорожная

карта” развития предлагаемых технических решений, качественно и понятно (пусть и только специалисту) описанные этапы разработки – признак того, что основатели стартапа действительно серьёзно подошли к делу и планируют реально довести проект до полноценного рабочего продукта.

- Наличие MVP (минимально жизнеспособного продукта). Пункт, вполне логично вытекающий из предыдущего. Дело тут даже не в возможном мошенничестве: администраторы HYIP-проектов, банальных пирамид, вряд ли смогут даже составить нормальное техническое описание и планы дальнейшего развития. Однако и среди реальных разработчиков блокчейн-систем, к сожалению, встречаются прожектёры – мол, запустим стартап, соберём инвестиций и будем писать код как получится. Когда дело доходит до реальной разработки, может оказаться, что уровень основателей проекта недостаточен для реализации намеченных планов. А вот наличие уже готового, пусть и “сырого”, но работающего продукта – весомый довод в пользу проекта. Конечно, этот MVP будет долго дорабатываться, пока не превратится в готовый и доступный пользователям продукт, однако именно для этой “доработки напильником” и собираются инвестиции.
- Общий бизнес-анализ. Стандартная процедура проверки компании перед покупкой акций (токенов) или вхождением в основной капитал проекта. Важная составляющая этой аналитики – изучение личностей основателей и основных разработчиков стартапа. Конечно, большинство этих людей не слишком известны в мире большого бизнеса, однако в профессиональной среде можно найти отзывы и прочую информацию, также не стоит игнорировать профили на Facebook и LinkedIn. Ну и не забывайте об обязательном исследовании юридической документации и бизнес-плана.
- Объективная и субъективная оценки перспективности. Самый, пожалуй, сложный критерий определения пригодности или непригодности стартапа для инвестирования. Тут всё зависит как от ваших знаний в данной сфере, так и от абсолютно личных предпочтений. Объективно перспективы развития конкретной технологической схемы можно оценить на профессиональных форумах, в сетевых сообществах, однако не забывайте, что это только прогнозы, пусть и от хорошо разбирающихся в этом экспертов отрасли.

Особенности национального блокчейна

Самая печальная часть статьи, к сожалению, однако от российской специфики никуда не денешься. Всё вышеописанное радужное состояние дел, увы, относится преимущественно к зарубежным блокчейн-стартапам и к IT-отрасли в целом. Проекты, зарегистрированные в России и рискнувшие выйти на ICO, упираются в мощную и практически непреодолимую стену, во многом связанную с общим состоянием дел в отечественной сфере высоких технологий – законодательство. Ныне действующие федеральные законы совершенно не регулируют такие относительно новые материи, как криптовалюты, токены и блокчейн-системы в целом. Активно обсуждаемый и исправляемый в Госдуме законопроект “О цифровых финансовых активах” также описывает распределённые реестры и основанные на них системы общими словами, не упрощая, а только запутывая разработчиков, пользователей и регулирующие органы власти.

Неудивительно, что самый успешный криптотехнологический стартап прошлого года MobileGo обернулся катастрофическим провалом и находится в состоянии полураспада – а ведь он собрал более 50 миллионов долларов на ICO. Существенных прорывов пока не наблюдается и у менее раскрученных проектов в области блокчейн-разработок. Пограничное с точки зрения закона положение этой отрасли плюс общая зарегулированность бизнес-среды приводит к тому, что подавляющее большинство перспективных стартапов с русскими корнями регистрируется и проводит ICO в странах с более дружелюбным инвестклиматом – на Кипре, в Израиле, Сербии и даже в Литве. Естественно, туда же идут и деньги крупных российских венчурных фондов.

В целом, инвестиции в блокчейн-проекты на ранней стадии развития сегодня могут оказаться такими же прибыльными, как вложения в середине-конце 1990-х годов в молодые компании “Яндекс” и Google или в середине 2000-х в никому не известный стартап Facebook. Блокчейн-технологии – будущее для целого класса сетевых платформ и систем безопасной обработки, хранения и использования информации. Однако не забывайте, что это в любом случае венчурные инвестиции, и риск того, что проект “не взлетит”, крайне высок. Вспомните, сколько десятков поисковиков конкурировали друг с другом в интернете всего 20 лет назад, и кто из них дожил до нынешнего времени. Конечно, покупка отдельных токенов новых компаний очень удобна, вы можете инвестировать в будущих интернет-гигантов достаточно небольшие суммы. Но спрогнозировать, какие именно из нынешних стартапов станут “яндексами” и “фейсбуками”, крайне сложно. Вкладывайтесь в несколько проектов, желательно с максимально различающимися продуктами, выбирайте объекты инвестирования с умом – и да пребудет с вами сила».

8.1.2. Материалы, анализирующие случай сети Кэшбери

В связи с идентификацией сети Кэшбери в качестве крупнейшей финансовой пирамиды осенью 2018 года такие материалы активно появляются практически во всех СМИ. Материалы интересны для работы над кейсом, поскольку представляют собой описание конкретного случая из новейшей практики.

- **Интерфакс – ЦБ назвал «Кэшбери» одной из самых масштабных выявленных финансовых пирамид**
  https://www.interfax.ru/business/630745

«Компаниям под брендом "Кэшбери" удалось вовлечь в свой проект несколько десятков тысяч человек

ЦБ РФ выявил явные признаки финансовой пирамиды в деятельности группы российских и иностранных компаний под единым брендом "Кэшбери", передал информацию о них в Генеральную прокуратуру РФ и МВД, говорится в сообщении регулятора.

Компании группы "Кэшбери" строят свою деятельность на принципах сетевого маркетинга, обещают завышенную доходность, ведут агрессивную рекламу в СМИ и социальных сетях. Деньги привлекаются и в рублях, и в криптовалюте, но при этом признаки реальной экономической деятельности отсутствуют, лицензии Банка России у компаний, которые предлагают финансовые услуги, нет.

По экспертным оценкам, "Кэшбери" удалось вовлечь в свой "проект" несколько десятков тысяч человек.

"Это одна из самых масштабных финансовых пирамид, которую мы выявили за последние годы, она развернула свою деятельность во многих регионах, практически по всей стране. Причем, в последнее время рекламирует себя все более активно, стараясь вовлечь как можно больше граждан", - сказал директор департамента противодействия недобросовестным практикам ЦБ Валерий Лях, слова которого передала пресс-служба ЦБ.

"Мы считаем необходимым предупредить граждан о рисках, связанных с вложением денег в этот "проект", чтобы уменьшить их возможный ущерб", - сказал Лях.

В 2015-2018 годах Банком России зафиксирована деятельность почти 600 организаций и интернет-проектов, имеющих признаки финансовой пирамиды. Материалы об их деятельности переданы в правоохранительные органы и прокуратуру».

- **РБК –**
  Почему десятки тысяч людей поверили финансовой пирамиде «Кэшбери»
  https://www.rbc.ru/finances/26/09/2018/5bab792c9a79473985b84349

«ЦБ выявил одну из самых масштабных финансовых пирамид за последние годы – «Кэшбери». Компания не ведет реальной экономической деятельности и активно себя рекламирует. Обещание доходности до 600% привлекло десятки тысяч человек.

Классическая пирамида

Банк России увидел «явные признаки» классической финансовой пирамиды в группе российских и иностранных компаний, действующих под единым брендом «Кэшбери», говорится в распространенном пресс-службой ЦБ комментарии директора департамента противодействия недобросовестным практикам Центробанка Валерия Ляха. Регулятор передал информацию о группе в Генпрокуратуру и МВД.

Компании группы «Кэшбери» строят свою деятельность на принципах сетевого маркетинга, обещают завышенную доходность, ведут агрессивную рекламу в СМИ и социальных сетях, говорит Лях. Деньги привлекаются и в рублях, и в криптовалюте. Между тем признаки реальной экономической деятельности отсутствуют, лицензии Банка России у группы компаний, которые предлагают финансовые услуги, нет.

«Это одна из самых масштабных финансовых пирамид, которую мы выявили за последние годы, она развернула свою деятельность во многих регионах, практически по всей стране», – отмечает Лях. По экспертным оценкам, которые приводит глава департамента ЦБ, «Кэшбери» удалось привлечь в свой проект несколько десятков тысяч человек. Причем в последнее время компания рекламирует себя все более активно, стараясь вовлечь как можно больше граждан, подчеркнул Лях.

Все эти факты были установлены сотрудниками Банка России в результате работы по противодействию нелегальной деятельности на финансовом рынке. «Мы считаем необходимым предупредить граждан о рисках, связанных с вложением денег в этот «проект», чтобы уменьшить их возможный ущерб», – отмечается в сообщении ЦБ.

Банк России передает информацию правоохранителям о нарушениях, как только удается установить или подтвердить факты, которые свидетельствуют о наличии в деятельности организации признаков финансовой пирамиды, уточнил в ответ на запрос РБК Валерий Лях. При этом проверяются все проекты, в отношении которых есть такие сигналы

(это могут быть как обращения граждан, так и агрессивная реклама в СМИ или соцсетях). В случае «Кэшбери» ЦБ получал сообщения о том, что деятельность компании «масштабировалась» по разным каналам, «в том числе от коллег в регионах», добавил директор департамента противодействия недобросовестным практикам ЦБ.

РБК направил запрос в «Кэшбери», однако ответа не получил. На звонки по номерам, указанным на сайте компании, в том числе по номеру «горячей линии», РБК никто не ответил.

Лондон и «Варшава»

Согласно информации на сайте организации, с 2016 года «Кэшбери» представляет собой группу компаний, в которую входит микрокредитная компания «Варшава», ООО «Кэшбери» (зарегистрированная в Ростове-на-Дону с фактическим адресом в Дубае) и зарегистрированная в Лондоне компания Cashbery International Limited, которая «координирует работу платформы для инвесторов». «В дальнейшем список компаний будет расширяться, в соответствии с развитием компании», – отмечается на сайте. В качестве председателя правления группы компаний «Кэшбери» указан Артур Варданян (он представлен как бывший руководитель кредитного отдела «в одном из крупнейших банков России»). Согласно данным британского реестра компаний, Варданян – директор Cashbery International Limited. Он же назван «собственником идеи и всех разработанных площадок и продуктов холдинга Cashbery ltd в Англии и ОАЭ». Руководителем и владельцем МКК «Варшава», согласно данным базы СПАРК, является Вадим Герасимов. Гендиректор и владелец МФО «Кэшбери» и ООО «Кэшбери» – Роман Алексеев.

Доходность в сотни процентов

В материалах Банка России названо несколько признаков, которые могут помочь распознать финансовую пирамиду. Среди этих признаков: отсутствие лицензии на осуществление деятельности по привлечению средств, обещание доходности в несколько раз выше рынка, а также ее гарантирование, агрессивная реклама в СМИ и интернете, отсутствие данных о финансовом положении компании, собственных средствах и точного определения деятельности организации. Кроме того, общий признак финансовых пирамид – выплаты новым участникам из тех денег, которые внесли вкладчики раньше.

Некоторые аспекты работы «Кэшбери» совпадают с перечисленными регулятором признаками. Компания предлагает клиентам «выдавать займы с доходностью до 600% годовых». Компания дает возможность «прокредитовать» частных лиц, малый и средний бизнес, предоставить финансирование под залог движимого и недвижимого имущества, а также инвестировать в криптовалюту. Выдавать микрозаймы физлицам предлагается с доходностью до 600% годовых (порог входа – 1 тыс. руб.), займы малому и среднему бизнесу – до 228,5%. (от 200 тыс. руб.). Через cashbery.com можно также взять заем под 1,2–2,2% в день, в зависимости от его суммы.

В информации о юридической модели группы компаний отмечается, что ООО «Кэшбери» не является микрозаймовой компанией, а с помощью инструмента «Площадка взаимного кредитования» «выстраивает процессы взаимодействия между инвесторами и заемщиками». При этом подчеркивается, что каждый инвестор и заемщик «действуют на свое усмотрение».

«Кэшбери» вело агрессивную рекламную кампанию в СМИ и интернете. В частности, на страницах «Кэшбери» в Youtube и «ВКонтакте» можно найти ролики, где на мероприятиях «Кэшбери» выступают певцы Николай Басков (он исполнил гимн «Кэшбери») и Валерий Меладзе. «Кэшбери» также рекламировали популярные видеоблогеры.

Без шансов на возмещение

Схемы, подобные тем, какими руководствовалась «Кэшбери», или придумываются изначально с целью мошенничества, или же собственники приходят к ним из-за неудач в бизнесе, говорит партнер FMG Group Михаил Фаткин. По его словам, в первом случае, как правило, на руководящие должности сразу назначаются только номинальные люди, а реальные собственники скрываются в тени. Во втором случае собственники пытаются хищение скрыть за обычной хозяйственной деятельностью. Схемы вывода денег основываются на длинной цепочке различных юрисдикций, чтобы затруднить в дальнейшем правоохранительным органам и кредиторам поиск конечного бенефициара, отмечает Фаткин. К ответственности для начала привлекут руководителей компании и собственников, и если они будут давать показания, то правоохранительные органы смогут выйти и на реальных бенефициаров, рассуждает юрист. К ответственности могут привлечь управленцев, которые не были в штате, но организовывали работу пирамиды: даже если конечный собственник не находится в России, то в России могли действовать его представители, которые инкассировали и выдавали деньги, вели переговоры с клиентами, говорит Фаткин.

Как правило, в полном объеме возместить финансовый ущерб не удается вкладчикам ни одной пирамиды, говорит партнер юридической фирмы «Рустам Курмаев и Партнеры» Дмитрий Горбунов. Высокий уровень защиты конечных бенефициаров пирамид, обусловленный их анонимностью и, наоборот, крайне низкий – для лиц, инвестирующих в них, – это проблема, которую сложно решить, подчеркивает он. По словам Горбунова, в теории жертвы пирамид могут обратиться в ЦБ или в Росфинмониторинг – такое обращение может быть действенным с точки зрения пресечения дальнейшей незаконной деятельности организации и привлечения ее бенефициаров к уголовной ответственности. Однако это никак не поможет инвесторам компенсировать убытки. Можно подать иск в адрес организации или ее бенефициаров, но на счетах пирамид, как правило, не оказывается средств даже для частичного покрытия убытков, добавляет юрист.

Масштабы проблемы

В 2015–2018 годах Банком России зафиксирована деятельность почти 600 организаций и интернет-проектов, имеющих признаки финансовой пирамиды, причем с начала 2018 года – 82 таких организации. Из выявленных в этом году пирамид больше половины (47) существовало в виде ООО, 16 было создано как интернет-проекты, 11 – как потребительские кооперативы, 5 – потребительские общества, две действовали как индивидуальные предприниматели, и одна финансовая пирамида была организована в форме акционерного общества.

Заметной тенденцией последнего года стало привлечение средств граждан в финансовые пирамиды, основанные на псевдоинвестициях в криптоактивы, говорил в июле Валерий Лях. И если в обычных финансовых пирамидах средняя сумма вложенных

гражданами средств составляет 30–40 тыс. руб., то в финансовые пирамиды на мнимых инвестициях в криптоактивы средняя сумма в 2,5 раза выше – около 100 тыс. руб.»

- **Forbes – Набрали кэша. ЦБ выявил «звездную» финансовую пирамиду** **http://www.forbes.ru/finansy-i-investicii/367339-nabrali-kesha-cb-vyyavil-zvezdnuyu-finansovuyu-piramidu**

«Банк России уличил компанию «Кэшбери» в признаках финансовой пирамиды, которая привлекала средства как в рублях, так и в криптовалюте. В ее рекламной кампании активно участвовали звезды российского шоу-бизнеса

Банк России передал в Генеральную прокуратуру и МВД информацию о группе российских и иностранных компаний, действующих под единым брендом «Кэшбери». Об этом передал через пресс-службу регулятора директор департамента противодействия недобросовестным практикам ЦБ Валерий Лях.

«Мы видим в их деятельности явные признаки классической финансовой пирамиды. Компании группы «Кэшбери» строят свою деятельность на принципах сетевого маркетинга, обещают завышенную доходность, ведут агрессивную рекламу в СМИ и социальных сетях. Деньги привлекаются и в рублях, и в криптовалюте, но при этом признаки реальной экономической деятельности отсутствуют, лицензии Банка России у компаний, которые предлагают финансовые услуги, нет», – говорится в сообщении Ляха.

По экспертным оценкам, «Кэшбери» удалось вовлечь в свой «проект» несколько десятков тысяч человек, уточняет представитель ЦБ. «Это одна из самых масштабных финансовых пирамид, которую мы выявили за последние годы, она развернула свою деятельность во многих регионах, практически по всей стране. Причем, в последнее время рекламирует себя все более активно, стараясь вовлечь как можно больше граждан», – следует из сообщения Ляха.

Примечательно, что в рекламной кампании «Кэшбери» отметились звезды российского шоу-бизнеса. Среди них – Николай Басков, который записал гимн компании и снимался в роликах в ее поддержку, популярная певица и ведущая Ольга Бузова – она советовала покупать криптовалюту «Кэшбери», а также певец Валерий Меладзе – на Youtube можно найти видео, где он поздравляет компанию с днем рождения.

Владелец ООО «Кэшбери» – Роман Алексеев, следует из данных СПАРК. Компания зарегистрирована в городе Ростов-на-Дону. На ее сайте указано, что в группу входят МФО «Варшава», МФО «Кэшбери» и английская компания «Cashbery Limited», координирующая работу платформы для инвесторов.

В 2015-2018 годах Банком России зафиксирована деятельность почти 600 организаций и интернет-проектов, имеющих признаки финансовой пирамиды, приводит статистику Лях. Материалы об их деятельности переданы в правоохранительные органы и прокуратуру.

ЦБ также активизировал борьбу с инсайдом на финансовом рынке. В августе 2018 года регулятор рассказал о многолетних манипулированиях (2012-2016 годы) близких к «Финаму» компаний – сделки совершались с акциями многих российских и иностранных эмитентов, среди которых UC Rusal и Polyus Gold.

В апреле 2018 года Банк России заявил о том, что вычислил схему манипулирования известным трейдером и инвестором Элвисом Марламовым в рамках сервиса «Автоследование». Прогнозируя торговое поведение своих «последователей», трейдер мог обогатиться на 8 млн рублей, утверждает Центробанк.

В ноябре 2017 года ЦБ рассказал о двух магнитогорских трейдерах Даниле Шейнине и Ирине Мулявко, которые, по данным регулятора, обманули Магнитогорский металлургический комбинат (ММК) на 89 млн рублей, занимаясь манипулированием его акциями на Московской бирже».

Отзывы и истории инвесторов Кэшбери дают представление о мотивах, которыми руководствуются люди при вложении в такие проекты, а также отношении инвесторов к последствиям идентификации финансовой пирамиды:

https://journal.tinkoff.ru/cashbery-lovers/;

https://life.ru/t/%D1%84%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D1%8B/1167423/keshbieri_zhivi_chiem_dieliatsia_v_sotssietiakh_zhiertvy_novoi_finansovoi_piramidy;

https://www.banki.ru/news/lenta/?id=10759861.

8.2. Обзорные материалы о тенденциях развития рынка криптовалют

Обратите внимание, что оценка перспектив и регулирование рынка криптовалют являются одними из наиболее дискуссионных тем цифровой экономики. Мы постарались это отразить в материалах Сборника.

- **Банк России – Обзор по криптовалютам, ico (initial coin offering) и подходам к их регулированию. Декабрь 2017. http://www.cbr.ru/Content/Document/File/36009/rev_ICO.pdf**

«Обзор содержит основные понятия в сфере использования технологии распределённых реестров, криптовалют и ICO в соответствии с международным опытом, основные аспекты выпуска и обращения криптовалют и проведения ICO, а также описание подходов к их регулированию в разных странах.

Итоги года для рынка криптовалют https://cryptorussia.ru/zametki/itogi-goda-dlya-rynka-kriptovalyut

Уходящий 2018 год стал настоящей проверкой рынка криптовалют на способность выдерживать новые удары по курсу. Тем не менее эксперты не склонны думать, что год был негативным. В целом, по их мнению, произошло много позитивных изменений, которые позволяют надеяться на позитивное будущее.

Курсы криптовалют

Почти все опрошенные Cryptorussia эксперты, подводя итоги года, приводят в качестве одного из главных событий - падение курсов криптовалют. По подсчетам журналиста и криптоинвестора Олега Чеботарева, в 2018 году стоимость активов упала в среднем на 80%. По мнению специалиста, это связанно с несколькими фундаментальными изменениями. Первое – ужесточения законодательства в крупнейших странах мира. Второе – потеря доверия «как между участниками криптовалютного сообщества, так и к токенам в целом». По мнению Олега Чеботарева, из-за мошенничества с рынка вместе с доверием ушли и деньги.

В качестве негативного момента снижение курса отметил и эксперт по финансовым технологиям Cryptocode Александр Лозбень.

«Этот год был сложным и эмоциональным для всех участников рынка. Я часто и у многих спрашивал, удалось ли им заработать на падении, и всегда ответ был отрицательный. Из этого могу сделать вывод, что для инвесторов этот год был негативный», – отмечает эксперт. Он также называет главным событием года – отток капитала с рынка.

Однозначно негативным годом 2018-й можно назвать только рассматривая его с точки зрения общей капитализации и курсов, считает юрист компании «Прифинанс» Артур Ибрагимов. В качестве главных событий он также называет:

- Выдачу лицензии для швейцарского Crypto Fund AG,
- Запуск платформы Fidelity Digital Asset,
- Формирование в ряде стран законодательства, регулирующего криптовалюты,
- Бойкот криптовалют со стороны крупных интернет-корпораций – запрет рекламы криптовалют, блокировка профильных аккаунтов в соцсетях и др,
- Выход на IPO ряда криптовалютных компаний.

Главным событием ведущий аналитик брокера RoboForex Дмитрий Гуровский называет падение доверия к сектору и сокращение объемов торгов.

«Майнеры увидели, что их доходы не всегда могут быть масштабными, а покупатели убедились в том, что без "свежих" денег сектор безнадежен», - говорит Дмитрий Гуровских.

Положительные итоги года

Несмотря на серьезные потери инвесторов, эксперты по разным причинам называют год скорее положительным, чем отрицательным. Журналист Олег Чеботарев указывает на очищение рынка от мошенников и случайных людей.

«Рынок оставил лишь тех юридических и физических лиц, которые точно представляют свои цели и знают что они делают в мире блокчейн технологий. Криптовалютный рынок находится в процессе очищения и в 2019 году он выйдет на активное развитие, стряхнув с себя накопившийся балласт», - говорит Олег Чеботарев.

Также эксперт отмечает, что не понимает, почему некоторые эксперты удивлялись краху той или иной криптовалюты. По его мнению, выжовут те, кто успел завоевать собственную нишу и представляет ценность для владельца.

Очищение рынка называет позитивным моментом и Александр Лозбень. По его версии, теперь на рынке налажен порядок и из него ушли те, кто не смог работать и зарабатывать в сложных условиях. Сами же криптовалюты не растеряли привлекательность и актуальность. Год «обрядом очищения» называет директор по развитию продуктов Zichain Тарас Чумаченко. Он отмечает, что майнинг, например, стал обычным бизнесом с адекватной маржинальностью, стоимостью услуг по разработке, маркетингу или юридическому сопровождению. Цены перестали быть сильно завышенными:

«Всё это является хорошим знаком трансформации и перехода блокчейн-индустрии к более зрелому состоянию»

Перспективы, по мнению эксперта, также хорошие так как государственные структуры постепенно начинают оказывать поддержку рынку.

Со-основатель BitCluster Сергей Арестов также называет коррекцию главным событием года, но не считает ее негативной.

«Конец 2018 года демонстрирует то, что неэффективность в данном виде бизнеса наказуема. Для эффективной работы в области майнинга крайне важна стоимость электричества. Кроме того, каждый день необходимо фиксировать намайненную валюту, вовремя выводить на биржу, переводить в USDT, правильно выбирать пулы, смотреть, по какому алгоритму лучше майнить, по какому принципципу- PPS или PPLNS- только совокупность всех этих факторов и грамотно выполненная работа может оставить майнинг выгодным»

Тем не менее эксперт считает, что год сохранит для разных участников рынка оценку – от сверхнегативного до сверхпозитивного. Если начало года было сверхдоходным, то после коррекции многие майнеры больше вообще не работают.

Положительным год считает и Артур Ибрагимов. По его словам, теперь рынок стал более цивилизованным:

«Я бы считал 2018 год позитивным, даже несмотря на сильную просадку курсов. Рынок стабилизируется, развивается, становится более цивилизованным. И все это не могло не привести к просадке курса. И более значительными мне видятся все же позитивные события и тенденции, о которых я написал выше».

- **ТАСС – Перспективы рынка криптовалют в 2018 году https://tass.ru/press-relizy/5252742**

«За каждым взлетом следует спад и к лету 2018 капитализация рынка приблизительно на 55% ниже, чем на историческом пике – в начале 2018

Прошлый 2017 год вспоминают, как период активнейшего up-тренда виртуальных, валют, ICO – выпуска новых токенов и развития инфраструктуры криптопространства. К сожалению, экономические закономерности отменить нельзя. За каждым взлетом следует спад и к лету 2018 капитализация рынка приблизительно на 55% ниже, чем на историческом пике – в начале 2018. Максимальное изменение составляло около 70% и пришлось на начало апреля 2018.

2018 год ICO

Как-бы устрашающе не выглядели цифры, коррекция для традиционных рынков в пределах 60% считается глубокой, но в пределах нормы. Криптовалюты гораздо волатильнее, чем акции, товары и индексы. Технически, цены нашли дно. На недельных графиках виртуальных активов формируется фигура, которая может превратиться в разворотную модель 3 вершины или голова-плечи. Завершение консолидации ожидается ближе к осени. На сегодняшний день график движения курса Биткоин находится в разнонаправленном тренде, а текущая стоимость в 7500$ является очень низкой.

В около криптовалютном пространстве жизнь продолжается. Анонсируются ICO, в числе которых проекты, оптимизирующие взаимодействие большого числа пользователей, чувствуют себя очень хорошо.

В этой отрасли предполагается рост.

4. Если мировой объем составил в 2017 3,2 млрд привлечённых в процессе ICO долларов, то прогноз на 2018 – 5 млрд, то есть на 55-60% больше.
5. В России в текущем году ожидается увеличение инвестирования стартапов более чем вдвое – 650 млн долларов против 300 млн в 2017.

В тоже время, откладывается выпуски, напрямую связанные с рыночными котировками. Так, биржа EXMO перенесла ICO на осень, поскольку ситуация сниженного спроса – плохой старт для токенов под цели маржинального кредитования.

Удельная доля плохих проектов по-прежнему велика. Чтобы не терять в будущих скамах деньги, необходимо в деталях проверять информацию о проекте, его команде и изучать мнение сообщества.

Курсовые тренды

На рынке криптовалют очевидна тенденция диверсификации, когда удельная доля биткоина снижается. Инвесторы знакомятся с отраслью и вкладывают средства:

- в фаворитов из TOP-10 рейтинга капитализации по версии Coinmarketcap;
- перспективные монеты из TOP-50;
- малоизвестные широкой публике активы.

Доля последних увеличилась за год более, чем втрое – с 7 до 25.

Из отдельных криптовалют ближе всего к биткоину Ethereum. При этом инвестиции в ETH отличаются крайней волатильностью – с начала 2018 были моменты, когда капитализация BTC и ETH отличалась между собой на 70% и более, чем на 300%.

К концу 2018 можно ожидать, что:

- Bitcoin будет занимать четверть доли рынка;
- Ethereum около 15%;
- Bitcoin Cash и Ripple по 10%;
- на активы из TOP- 50 придётся от 25% и выше;
- на остальные до 15%.

Перераспределение вкладов – тенденция, которая продолжится.

Если более детально изучить структуру распределения капитала на рынке криптовалют, то становится понятно, что рост капитализации монет за пределами TOP-10 – единственный восходящий тренд в этой области.

Политическая адаптация

Со стороны государственных юрисдикций продолжится регулирование криптовалют. Здесь все неоднозначно, одни страны открывают двери новой технологии, другие остаются в стороне, третьи отвергают.

1. Нейтральны – США, Индия, Россия, Нигерия, Гана.
2. Позитивны – Канада, Венесуэла, Япония, Сингапур, Австралия, Швейцария, Южная Африка.
3. Негативны – Китай, Южная Корея, ЕС.

Нейтрально отношение перечисленных стран довольно условно – представители властей делают заявления, оглашают планы и намерения. Предпринимаемые шаги направлены на определение финансовой сущности криптовалют, разработку правил проведения ICO, вопросы налогообложения. То есть нейтральные юрисдикции склонны двигаться в позитивном направлении.

Резюме

Возможно, но маловероятно, что криптовалюты протестируют в 2018 году исторические максимумы. Шансы на частичное восстановление гораздо выше, вполне достоверно выглядит цифра 50% от текущих уровней, что будет соответствовать 600 млрд долларов капитализации всего рынка».

- **Известия – Инвестиции в российские стартапы в криптовалюте выросли в 10 раз**
  https://iz.ru/687939/grigorii-kogan/investitcii-v-rossiiskie-startapy-v-kriptovaliute-vyrosli-v-10-raz

«Предприниматели оценили простоту привлечения суррогатных денег

Инвестиции криптовалют в российские стартапы за прошедший год выросли в десять раз и составили около $200 млн. Такие данные предоставили «Известиям» на торговой площадке CryptoBazar. Эксперты объясняют динамику тем, что на биржах денежных суррогатов нет жесткого регулирования. Средства там привлечь проще, чем традиционными способами. Однако у этой медали есть оборотная сторона: инвестор меньше защищен.

Начинающие предприниматели в России испытывают трудности с привлечением средств в свой бизнес: банки неохотно дают кредиты под высокорискованные проекты, а венчурные инвесторы выдвигают невыгодные условия. В связи с этим, а также на фоне роста популярности криптовалют, стартаперы всё больше развивают свои проекты с помощью ICO (привлечением инвестиций в цифровых деньгах, Initial Coin Offering).

– Банковские кредиты фермерам выдают с трудом. А если дадут, то очень дорого – к примеру, козу куплю, а дом отберут. А после ICO я рассчитываюсь своей продукцией и обеспечен клиентами, – рассказал «Известиям» фермер, автор ICO-проекта «Экосистема Колионово» Михаил Шляпников.

Он запустил свою криптовалюту – колионы – и в апреле прошлого года провел под них ICO. В итоге фермер получил в пересчете на доллары $510,5 тыс. от 103 участников. Теперь он поставляет саженцы, картофель и мясо птицы в счет выпущеных «денег».

– Российские предприниматели привлекли со всего мира в свои проекты в 2017 году инвестиций в криптовалютах более чем на $200 млн. А годом ранее было $20 млн. Стартаперы из России запустили более ста проектов в криптовалюте, а в 2016-м их было порядка 20, – рассказал основатель торговой площадки CryptoBazar и одноименного фонда Олег Иванов.

СПРАВКА «ИЗВЕСТИЙ»

При проведении ICO бизнесмен регистрирует компанию, описывает свой проект, запускает сайт и оповещает об этом потенциальных инвесторов по электронной почте.

Сейчас, по экспертным оценкам, каждое пятое ICO сделано выходцами из России. В общей сложности за последние четыре года команды из нашей страны собрали более $260 млн – 11% от общей суммы всех размещений. Среди таких проектов: суперкомпьютер SONM ($42 млн), «Русская майнинговая компания» (RMC) ($45 млн), мобильная игровая платформа MobileGo ($53 млн). Есть и производственные проекты. Например, промышленный стартап по производству синтетического диоксида циркония ZrCoin ($4,5 млн).

Вырос и средний возврат вложений – до 30 000%. Такая прибыльность связана с ростом курса крипловалют и повышением интереса к этой сфере, пояснил глава фонда. Если за четыре последних года компании могли привлечь через ICO в среднем на один крупный проект $2 млн, то по итогам 2017 года этот показатель достиг $22,6 млн. Однако высокая доходность всегда сопряжена с высокими рисками.

– Поскольку криптовалюта сама по себе – рискованная сфера, то привлечение инвестиций в ней – это риск в кубе. Вложения в проекты на ранней стадии в принципе не дают никаких гарантий прибыли. А тут еще и привлекаются средства в криптовалюте, цена которой крайне изменчива. Тут может быть как плюс тысячи процентов, так и минус. Поэтому как бы ни было хлопотно и дорого уже существующее IPO (первичное размещение акций), ICO их не заменят, – предупреждает сооснователь международного криптобанка Wirex Дмитрий Лазаричев.

Другой фактор – отсутствие в России законодательства об ICO, криптовалютах и блокчейне. Когда нет ограничений, у инвесторов развязаны руки. Но их вложения при этом защищены меньше, а владелец бизнеса оказывается в более сильной позиции. При этом в России сих пор не решен вопрос о налогообложении сделок, совершаемых с криптовалютой.

В ряде других стран уже определились с подходом к налогообложению ICO. Например, Белоруссия вообще отказалась взимать сборы с таких сделок, став своеобразным «криптовалютным офшором». В Японии денежные суррогаты признают платежным средством, а в США к ним относятся как к финансовому инструменту. Попытки ввести налогообложение этой сферы в настоящее время предпринимает Швейцария. В Федеральной налоговой службе РФ на вопрос «Известий» по поводу налогового статуса ICO отвечать не стали.

Сейчас в Минфине и Центробанке разрабатывают законодательство, регулирующее ICO и криптовалюты. В разработанном проекте документа пока лишь даны определения ICO, криптовалюты и других терминов, касающихся этого рынка, чтобы в спорных ситуациях можно было обращаться в суд. Вопрос налогообложения сделок в криптовалютах пока не прорабатывался.

Капитализация рынка криптовалюты по сравнению с привычными финансовыми рынками пока невелика – всего $0,6 трлн против $73 трлн на фондовом рынке. Но у «денежных суррогатов» есть высокий потенциал роста – многие инвесторы входят на рынок через биткоин, растет число блокчейн-сетей, а размер привлекаемых средств

увеличивается.

8.3. Подходы к регулированию рынка криптовалют

Здесь представлены обзоры о подходах к регулированию рынка криптовалют в России и в иных странах мира. Обратите внимание, что эти подходы только формируются, поэтому очень различны и динамичны».

- **Finanz.ru – Криптовалюты эффективнее традиционных инструментов, но необходимо регулирование – эксперты**
  https://www.finanz.ru/novosti/aktsii/kriptovalyuty-effektivnee-tradicionnykh-instrumentov-no-neobkhodimo-regulirovanie-eksperty-1027877450

«Использование криптовалют позволит сделать многие процессы и инструменты на финансовом рынке более эффективными, но для этого необходимо четкое регулирование, считают опрошенные ТАСС эксперты.

Ранее на этой неделе в рамках Гайдаровского форума замминистра финансов РФ Алексей Моисеев заявил, что больше не видит угрозы создания финансовой пирамиды с помощью криптовалют из-за падения их стоимости. Накануне на пленарном заседании форума премьер-министр РФ Дмитрий Медведев говорил о том, что считает необходимым внимательно наблюдать за ситуацией с криптовалютами, курс которых показал большую волатильность. Глава кабмина при этом подчеркнул, что такая волатильность криптовалют «не повод их «хоронить».

По мнению экспертов, положительный настрой правительства РФ в отношении криптовалют может быть связан с тем, что криптовалютный «пузырь» сошел на нет, а опыт других стран в использовании этого инструмента дает обнадеживающие результаты.

«Я думаю, что интерес к криптовалютам сейчас связан с тем, что пузырь на рынке уже лопнул. Криптовалюты - уже не «хайп», а нормальный инструмент, криптовалюты -

интересный актив. Правительство РФ видит, что другие страны от них не отказываются, а разрабатывают законодательство и учатся работать с ними», - отметила независимый финансовый советник Наталья Смирнова.

Начальник отдела анализа рынков альтернативных инвестиций ИК «Велес Капитал» Алексей Пикуза уверен, что в работе с криптовалютами угроз не больше, чем и в классических фиатных валютах. «В основном это борьба с криминальными активами и угроза мошеннических действий. Учитывая молодость направления и отсутствие опыта у рядового пользователя, мошенникам проще работать в данном сегменте. В процессе более массового использования и четкого регулирования данные угрозы будут значительно уменьшены», - добавил он.

Перспективы использования

Прежде всего, следует разделять обеспеченные и необеспеченные криптовалюты, говорят эксперты. «Обеспеченные криптовалюты - это финансовые активы, такие как ценные бумаги или, например, цифровые токены, которые планируется выпускать в Сингапуре в соответствии с законом о ценных бумагах и фьючерсах (SFA). У меня есть большие сомнения о том, что у нас в стране в ближайшее время найдется какое-то применение необеспеченным криптовалютам, ценообразование на которые формируется только на основании спроса. Для обеспеченных криптовалют то или иное применение будет найдено», - комментирует директор по инновациям Национального расчетного депозитария (НРД) Артем Дуванов.

По его словам, одной из областей применения обеспеченных криптовалют может быть обслуживание корпоративных клиентов банками при проведении расчетов. «В таких ситуациях могут применяться так называемые токенизированные рубли, чтобы сделать процесс быстрее и дешевле», - добавил эксперт.

«Технология блокчейн уже активно используется в РФ. Одно из направлений данной технологии, а именно криптовалюты, постепенно входят в нашу жизнь. Думаю, что появление крипторубля - не такая уж фантастическая перспектива», - соглашается Пикуза.

Ранее председатель комитета Госдумы по финансовому рынку Анатолий Аксаков заявил журналистам о том, что крипторубль может появиться в России в перспективе двух-трех лет. По его словам, крипторубль может быть обеспечен депозитами в традиционных рублях в уполномоченных кредитных организациях. Таким образом, криптовалюта будет отличаться от классического рубля только тем, что она обращается на блокчейне.

«Обеспеченные криптовалюты используются для повышения эффективности уже существующих процессов или инструментов или для создания новой инфраструктуры для новых процессов. При помощи токенов это делается зачастую быстрее и дешевле», - комментирует Дуванов.

Кроме того, токены используются в целях увеличения и расширения потока инвестиций в те или иные проекты. По словам эксперта, новые инструменты, которые сейчас начнут появляться на блокчейне, будут использовать эту технологию не потому, что их можно сделать только на блокчейне, но просто потому, что это гораздо удобнее.

Регулирование

Основной камень преткновения в вопросе функционирования криптовалют в России - регулирование. По словам экспертов, принятие соответствующих законов затягивается и процесс интеграции криптовалют в финансовую систему идет очень медленно.

«В США криптовалюты уже приравнены к ценным бумагам. В России пока только готовится к принятию законопроект о так называемых «цифровых финансовых активах», к которым хотят отнести криптовалюту и токены», - отмечает аналитик ИК «Фридом Финанс» Анастасия Соснова. По ее словам, для комфортного существования криптовалют в России не хватает законодательно закрепленных правил работы и надзора.

«Прежде всего нужно четкое понимание того, что такое криптовалюты. Необходимо, чтобы они однозначно были признаны финансовым активом, а не товаром, и не облагались НДС. Чтобы была четкая инфраструктура криптовалютного рынка, такая же, как на фондовом рынке, - депозитарий, биржа. Чтобы было понимание основных игроков рынка, которые имели бы нормальную лицензию в отличие от форекс-брокеров с отозванными лицензиями, которые вели свою деятельность не в России, а выводили деньги в иностранные юрисдикции», - поясняет Смирнова.

По ее мнению, все данные по работе с клиентами должны протоколироваться и регулироваться в рамках 115 Федерального закона. «А также, в соответствии с законом о финансовом консультировании, если неквалифицированный инвестор собирается работать с криптоактивами, нужно будет так же, как и в проекте о краудфандинге, придумать какую-то сумму, которую можно на свой страх и риск инвестировать в криптовалюты, а все что выше потребует от клиента подписи о том, что он осведомлен о рисках», - заключила она.

Все страны так или иначе пытаются регулировать криптовалюты, говорят эксперты. Основной вопрос - легальный и прозрачный переход из фиатных, традиционных денег в цифровые и обратно, с полным контролем происхождения активов для избежания незаконной деятельности. «Учитывая сложность данного процесса и «запятнанное» прошлое криптовалют, законодатели очень осторожно и неспешно подходят к вопросу регулирования. Позиция РФ пока достаточно консервативная, но работа по созданию законодательной базы не прекращается», - добавляет Пикуза.

Госдума в январе - феврале рассмотрит законопроекты о цифровой экономике, в том числе проект о цифровых финансовых активах, сообщал Аксаков на пресс-конференции в ТАСС. По его словам, долгожданный закон о цифровых финансовых активах находится в ГПУ на согласовании. Он идет в связке с двумя другими: закон о регулировании инвестиционных платформ, или о краудфандинге, и изменения в Гражданский кодекс.

О законопроекте

В мае 2018 года Госдума приняла в первом чтении законопроект о цифровых финансовых активах. Документ был инициирован группой депутатов Госдумы и членов Совета Федерации во главе с Аксаковым.

В той редакции законопроект предусматривал только один вид сделок, которые смогут совершать владельцы цифровых финансовых активов (в соответствии с законопроектом, к ним относятся криптовалюты и токены), - это сделки по обмену токенов на рубли или иностранную валюту.

Предполагалось, что законопроект введет определение цифровых финансовых активов, к которым относятся криптовалюта и токен, а также законодательно закрепит новый вид договора, заключаемого в электронной форме, - смарт-контракт, исполнение обязательств по которому осуществляется с использованием цифровых финансовых технологий.

Согласно тексту документа, принятого в первом чтении, криптовалюта и токен являются имуществом. В законопроекте определены ключевые различия между криптовалютой и токеном на основе признака одного эмитента (токен) и множества эмитентов/майнеров (криптовалюта), а также цели выпуска. Согласно законопроекту, цифровые финансовые активы не являются законным средством платежа на территории РФ».

- **Коммерсант – Деньги, которые не любят тишину**
  https://www.kommersant.ru/doc/3407834

«Госрегулирование не успевает за ростом криптовалютного рынка

Одна из самых популярных тем массового интереса в последние месяцы – криптовалюты. Неуклонно стремится вверх их стоимость. Стартапы, предлагающие инвесторам вложить в их развитие виртуальные монеты, растут как грибы. Финансовые регуляторы ведущих стран уже высказали свою позицию, не всегда положительную, в отношении новых финансовых активов. Заметно потеплело отношение российских чиновников к этому рынку – разрабатываются законопроекты, вводятся учебные курсы. Однако на скорое появление крипторубля рассчитывать не приходится.

Зарегулируй это

Когда-нибудь 2017 год назовут годом биткойна в России. Криптовалюты прочно заняли лидерские позиции в финансовой повестке. По данным «Медиалогии», количество упоминаний слова «криптовалюта» в российских СМИ с 1 января по 31 августа 2017 года выросло почти в семь раз – с 3 тыс. до 20,4 тыс. Интерес русскоязычного сегмента пользователей интернета к теме зафиксировали и в Google. Согласно статистике компании, рост поисковых запросов по видам криптовалют с начала года составил 560%, по запросу bitcoin – 220%, по ethereum – 760%. Термин «криптовалюта» в первом полугодии вошел в топ-100 самых популярных запросов Google со словами «что такое», причем 13-е место среди всех запросов с этими словами занял поисковый запрос «Что такое майнинг?».

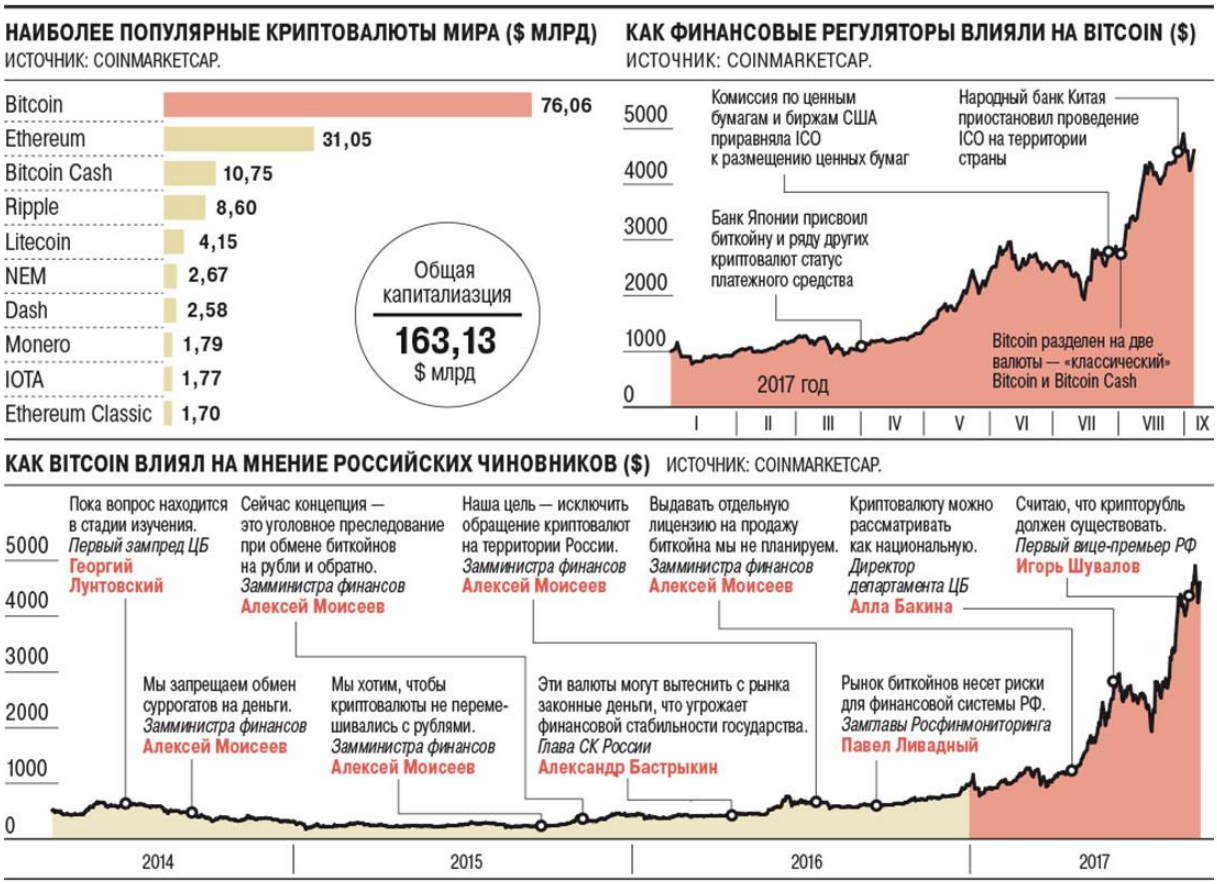
Взрывной рост всеобщего интереса к теме наглядно иллюстрирует и динамика курсов двух самых популярных криптовалют. За восемь месяцев текущего года курс биткойна вырос на 360%, достигнув 1 сентября исторического максимума ($4950,72). Курс второй по популярности криптовалюты – эфира (ethereum) – рос еще более впечатляющими темпами – с начала года плюс 3362%. На 31 августа рыночная капитализация биткойна превысила $76 млрд, совокупная стоимость всех криптовалют – $170 млрд. Выражаясь терминологией молодого рынка, криптовалютная тема сейчас находится на самом пике хайпа (от англ. hype – навязчивая реклама, шумиха, ажиотаж).

А еще совсем недавно отрасль была маргинальной и нишевой. За исключением ряда консервативных стран, установивших полный запрет на обращение и использование криптовалют, в течение нескольких лет мировое сообщество только присматривалось к новой финансовой сущности. 2017 год стал революционным: впервые со стороны

финансовых регуляторов ведущих стран мира прозвучали внятные заявления относительно криптовалютного рынка. 1 апреля Банк Японии присвоил биткойну и нескольким другим криптовалютам статус платежного средства наравне с иеной. 27 июля Комиссия по биржам и ценным бумагам США (SEC) приравняла первичное размещение токенов (initial coin offering, ICO, привлечение средств в криптовалюте) к размещению обычных ценных бумаг. 4 сентября Народный банк Китая заявил о приостановлении всех текущих ICO на территории страны, признав их незаконными. И криптовалютные рынки полноценно отыгрывали эти новости (см. график).

В России ситуация выглядит не более определенной, чем в других странах. Однако риторика чиновников за последние три года заметно поменялась – от полного неприятия самой идеи «альтернативных денег» чиновники постепенно переходят к картине управляемого криптовалютного рынка. В начале 2014 года ЦБ опубликовал информационное письмо, в котором рекомендовал участникам рынка воздержаться от использования криптовалют, так как они «могут быть, в том числе непреднамеренно, вовлечены в противоправную деятельность». Такую же позицию подтвердил и Росфинмониторинг. В октябре 2015 года Минфин разработал поправки к Уголовному кодексу, предусматривающие наказание в виде тюремного заключения за использование денежных суррогатов. Но к 2017 году чиновники уже пришли к выводу о необходимости создания в России системы регулирования криптовалютного рынка, разработкой соответствующего пакета законов занялась межведомственная рабочая группа по оценкам рисков оборота криптовалюты при Госдуме.

За последний месяц новостной фон вокруг криптовалютной темы стал невероятно насыщенным. В конце августа первый вице-премьер Игорь Шувалов заявил, что «крипторубль должен существовать», замминистра финансов Алексей Моисеев предложил разрешить биржевые операции с криптовалютами квалифицированным инвесторам. В начале сентября руководитель рабочей группы при Госдуме Элина Сидоренко сообщила об открытии при МГИМО курса «Правовые основы регулирования блокчейн-технологий», частью которого станут вопросы, связанные с оборотом криптовалют в РФ. Рынок ждал сформулированной позиции ЦБ. Однако результат оказался неожиданным – регулятор лишь подтвердил то, о чем говорил три года назад: «Банк России считает преждевременным допуск криптовалют к обращению и использованию на организованных торгах и в расчетно-клиринговой инфраструктуре на территории РФ».



«Даркнет или нет?

Темпы роста молодого рынка значительно опережают его внедрение в законодательные базы государств. И опасения чиновников понятны. Пожалуй, впервые за последние 30 лет они имеют дело с совершенно необычной сущностью, которую трудно держать под контролем, практически невозможно запретить и которая несет в себе вполне осязаемые риски. Главное опасение властей – отсутствие возможности мониторить и контролировать операции с криптовалютами, а также идентифицировать их инициаторов. А это – прямая угроза прогрессивного роста нарушений антиотмывочного законодательства. Впервые арест за отмывание средств при помощи криптовалюты состоялся еще в феврале 2014 года в США. Сообщалось, что криптотрейдерам Паскалю Рейду и Мигелю Эспинозе может грозить наказание в виде лишения свободы на 25 лет. В конце июля 2017 года в Греции был арестован российский гражданин Александр Винник по подозрению в отмывании средств через биржу BTC-e на сумму $4 млрд. В начале сентября МВД России сообщило о задержании в Костроме троих подозреваемых в ведении незаконной банковской деятельности – «организации виртуального обменного сервиса», служившего для обналичивания биткойнов за комиссионную плату.

При этом профессиональные «прачечные» постоянно совершенствуются. С одной стороны, по данным исследовательской компании Blockchain Intelligence Group, использование биткойна для совершения незаконных сделок сокращается. С другой – теперь преступники переходят на другие криптовалюты (в частности, monero и ethereum), трансакции которых сложнее поддаются мониторингу. Компания Chainalysis оценила доход от незаконных операций с валютой ethereum за семь месяцев 2017 года в $225 млн. И речь идет не только об отмывании, но и о других операциях криминального характера. Широкое распространение в последнее время получил «облачный майнинг». «Большая

часть проектов, которые предлагают начать инвестировать в майнинг от $100, являются стопроцентными пирамидами, где прибыль участники проекта получают исключительно за счет новых вкладчиков, а физических мощностей для майнинга проект не имеет»,– поясняет сооснователь блокчейн-сервиса по распознаванию и анализу речи Anryze Михаил Ежов. Кроме того, продолжает эксперт, растет число «бирж-кухонь», ничем не отличающихся от аналогов, известных по рынку Forex. Эти псевдобиржи не имеют реального стакана, а график зачастую копируется с другой биржи или просто рисуется.

Криптовалюты потенциально способны нарушить и некоторые устоявшиеся правила на финансовом рынке. Так, в теории, под угрозой может оказаться расчетная функция банковской системы. «Под влиянием крипторынка банки либо эволюционируют, либо перестанут существовать. В своем нынешнем состоянии банковская система выгодна в основном регулятору, так как он использует банки как своих агентов для противодействия отмыванию денег»,– считает управляющий партнер венчурного фонда AddVenture Алексей Прокофьев. По его словам, участники рынка криптовалют с помощью новых технологий предоставят регулятору более простой способ взаимодействия с рынком и станут альтернативой банкам. В то же время блокчейн и крипторынок не смогут полностью заменить банки с их сетью по идентификации, базой данных, платежными инструментами и способами оплаты (как в онлайне, так и в офлайне), указывает гендиректор платежного шлюза Fondy Андрей Воронин. «Технология блокчейн и банки должны работать в синергии. Точкой ввода и вывода наличных и безналичных денежных средств в любом случае всегда будет банк либо финансовый институт»,– считает он.

И мировые финансовые институты все активнее объединяют свои усилия с целью завоевать нишу на молодом рынке. 1 сентября Financial Times сообщила о новом этапе проекта по созданию «монеты для расчетов» (utility settlement coin, USC), в ходе которого к разработкам присоединились шесть крупнейших мировых банков – Barclays, Credit Suisse, Canadian Imperial Bank of Commerce, HSBC, MUFG и State Street. Ранее в проект вошли UBS, Deutsche Bank, Banco Santander, BNY Mellon и NEX. Участники заявили о своих планах запустить криптовалюту уже в 2018 году.

В России крупнейшие финансовые институты объединились в конце 2016 года в рамках ассоциации «ФинТех», созданной по инициативе ЦБ. Ассоциация занимается разработками в области технологии распределенных реестров, причем криптовалюты не являются их приоритетным направлением. Впрочем, в начале июня этого года зампред ЦБ, председатель наблюдательного совета ассоциации «ФинТех» Ольга Скоробогатова анонсировала начало работы над созданием национальной криптовалюты – крипторубля. Пока новостей об этом проекте немного. Скорее всего, засвидетельствовать хайп вокруг крипторубля можно будет не ранее 2018–2019 годов».

Как регулируется рынок криптовалют в разных странах мира

	Описание	Возможные положительные последствия	Возможные отрицательные последствия	Примеры стран
Отсутствие регулирования	Осуществляется наблюдение со стороны регулятора, информирование граждан о рисках участия в обороте криптовалют; Обращение и использование криптовалют не регламентируется и не регулируется	Отсутствие сигнала регулятора о привлекательности криптовалют как инвестиционного инструмента; Отсутствие ответственности регулятора за последствия реализации рисков, связанных с высокой волатильностью	Невозможность мониторинга движения средств и контроля за операциями, а также идентификации в целях ПОД/ФТ; Рост числа недобросовестных и мошеннических схем; Невозможность арбитража финансовых споров в правовом поле; Неконтролируемый рост оборота виртуальных валют	Индия, Бразилия, Аргентина, Австрия, Бельгия, Швеция, Дания, Эстония, Южная Корея, Российская Федерация. Как правило, отсутствие регулирования не является позицией регулятора и носит временный характер на период изучения и анализа до принятия решения о сценарии регулирования
Запрет	Полный запрет на обращение и использование криптовалют	Устранение угрозы стабильности национальной валюты со стороны криптовалют; Отсутствие рисков для потребителей; Минимизация рисков оттока средств, отмывания денег и финансирования терроризма	Увеличение теневого оборота средств; Вывод операций с криптовалютами в иные юрисдикции; Потенциальный отток специалистов и предпринимателей в сфере блокчейн и криптовалют за рубеж	Бангладеш, Боливия, Вьетнам, Исландия, Киргизия, Эквадор, Египет
Регулирование	Регистрация (лицензирование) обменных площадок, идентификация пользователей в целях ПОД/ФТ (может быть в соответствии с лимитами), налогообложение участников оборота, предоставление отчетности по операциям площадками, требования к минимальному капиталу площадок (опционально), защита прав потребителей, ответственность за нарушение установленных требований	Получение статистики по использованию криптовалют и мониторинг практик применения; Контроль операций и идентификация в целях ПОД/ФТ; Возможность введения ограничений на объемы и перечень операций; Возможность арбитража в рамках регулирования и установления ответственности	Легализация криптовалют может повысить интерес граждан к вложениям в криптовалюты и потенциально увеличить риски потери средств; Возможность использования недобросовестных и мошеннических схем и появления теневого оборота средств (в случае мер на уровне рекомендаций)	**Регулирование на основе НПА:** Китай*, Япония, Филиппины, Канада*, Швейцария, отдельные штаты США* (Вашингтон, Нью-Йорк); **Регулирование на основе рекомендаций (обязательный характер в части налогов):** Великобритания, Австралия (подготовлен законопроект), Сингапур*, Европейский союз (Франция, Германия и др.)

- **Ruscoins.info – Какие законопроекты о криптовалюте будут приняты Госдумой весной 2019 года? https://ruscoins.info/news/kakie-zakonoporoekti-o-kriptovalyute-budut-prinyati-vesnoy-2019-goda/**

«Принятие законов, посвященных регулированию цифровой экономики, является одним из приоритетов в законотворчестве – обозначил председатель Госдумы Вячеслав Володин на первом пленарном заседании.

Правительство РФ внесет более 20 законопроектов по вопросам цифровой экономики, 3 из которых были обозначены в докладе во время пленарного заседания. Каков правовой статус криптовалюты в России на начало 2019 года и принятие каких законов следует ожидать весной?

Содержание

- Правовой статус криптовалюты в России в 2019 году
- Законопроект «О цифровых финансовых активах»
- Законопроект «О внесении изменений в ГК РФ» («О цифровых правах»)
- Законопроект «О краудфандинге»
- Законопроект «Об экспериментальных правовых режимах в сфере цифровых инноваций»
- Законопроект «О совершении сделок с использованием электронной платформы»

Правовой статус криптовалюты в России в 2019 году

Летом 2017 года Правительство РФ утвердило программу «Цифровая экономика Российской Федерации». Программа рассчитана до 2024 года, общая стоимость проектов оценивается в 1,8 трлн. рублей, из которых 1,5 млрд. рублей выделены на совершенствование нормативной базы в сфере цифровой экономики.

Цели введения программы – создание экосистемы цифровой экономики РФ, условий для развития высокотехнологических бизнесов и повышение конкурентоспособности экономики РФ на глобальном рынке. Цифровая экономика представлена тремя уровнями: рынки и отрасли экономики, платформы и технологии и среда. К одной из основных цифровых технологий, обозначенных в программе, относится система распределенного реестра (в том числе, блокчейн). Однако, несмотря на финансирование программы, блокчейн и криптовалюта по-прежнему не закреплены в законодательстве РФ. Однако ряд законопроектов в области цифровой экономики готов к принятию уже весной 2019 года.

Законопроект «О цифровых финансовых активах»

Обсуждение законопроекта «О цифровых финансовых активах» (далее – «О ЦФА») началось весной 2018 года. Но он по-прежнему не принят из-за разногласий в подходах к определению основных понятий: «майнинг», «криптовалюта» и «токен». В первой редакции законопроекта майнинг был определен как добыча криптовалют. Затем законодатель решил определить майнинг как выпуск токенов для привлечения инвестиций. В первой редакции было разграничение между криптовалютой и токеном. Под «криптовалютой» понимался цифровой финансовый актив на блокчейне. Под «токеном» –

цифровой финансовый актив, выпущенный юридическим лицом или индивидуальным предпринимателем с целью привлечения денежных средств. В обновленной редакции исчезло определение «криптовалюта», но остались токены как средство инвестиций.

Из-за отсутствия единогласия и конфликтов с действующим законодательством было принято решение вернуть законопроект «О ЦФА» в стадию первого чтения. Принятие закона следует ожидать весной. Законопроект призван обозначить основные определения в области криптовалюты, закрепить права потенциальных инвесторов и оградить их от возможных рисков. Закон «О ЦФА» будет призван регулировать выпуск токенов, их обмен через специально созданных операторов обмена финансовых активов, закрепит описание договора «смарт-контракт» и установит правила ICO.

Законопроект «О внесении изменений в ГК РФ» («О цифровых правах»)

Вячеслав Володин обозначил в своём докладе принятие законопроекта «О цифровых правах». Новый закон призван закрепить в гражданском обороте определение «цифрового права» и «цифровых денег». К началу 2019 года из-за отсутствия закрепленного правового регулирования криптовалюта в России фактически находится вне поля защиты. То есть, в случае хищения кошелька или приобретения токенов недобросовестных компаний, граждане не могут рассчитывать на правовую защиту. Придав криптовалюте статус имущества, её можно будет учитывать в конкурентной массе должника, а также при разделе совместно нажитого имущества супругов. Однако законодатель РФ исходит из позиции, что криптовалюта не является законным средством платежа. Криптовалюта – это инвестиции, но не деньги.

Законопроект «О краудфандинге»

Также в своём выступлении Вячеслав Володин упомянул законопроект «О краудфандинге», напрямую не связанный с криптовалютами. Однако законопроект «О краудфандинге» предусматривает правовую защиту использования смарт-контракта и токенов в краудфандинге (инвестировании средств на инвестиционных платформах). Новая редакция закона «О краудфандинге» устанавливает максимальную сумму инвестиций для неквалифицированных инвесторов через краудфанинговые платформы в размере 600 000 рублей в год.

Законопроект «Об экспериментальных правовых режимах в сфере цифровых инноваций»

Минэкономразвития выступило с инициативой создать особый правовой режим, так называемые, «песочницы», в которых будут обкатываться новые технологии. Необходимость в таких «песочницах» обусловлена действующим законодательством. Развитие цифровой экономики тормозится отсутствием правовых норм и длительностью их принятия. Поэтому предлагается создать координационные и регулирующие органы, которые в содействии с юридическими лицами, индивидуальными предпринимателями и органами власти могли бы проверять инновации и отсеивать неработающие модели. Собственная «песочница» была запущена центральным банком России в апреле 2018, а в сентябре 2018 на её базе успешно состоялось тестовое ICO.

Законопроект «О совершении сделок с использованием электронной платформы»

Законопроект предусматривает регулирование создания и особенности использования так называемых «маркетплейсов» – электронных платформ. Маркетплейсы будут созданы для предоставления брокерских, страховых и финансовых услуг гражданам со множеством организаций в рамках одной платформы. Оператором маркетплейса сможет стать юридическое лицо в форме хозяйственного общества, с минимальным размером оборотных средств в 100 млн. рублей. Создание электронных платформ предусматривается законопроектом «О цифровых финансовых активах». Через такие платформы граждане смогут осуществлять сделки с криптовалютой. Запуск электронной платформы запланирован на февраль 2019 года».

С текстами и ходом обсуждения законопроектов можно ознакомиться на официальном сайте Государственной Думы по следующим ссылкам:

- Законопроект № 419059-7 О цифровых финансовых активах: http://sozd.duma.gov.ru/bill/419059-7,
- Законопроект № 419090-7 О привлечении инвестиций с использованием инвестиционных платформ (первоначально законопроект носил название "Об альтернативных способах привлечения инвестиций (краудфандинге)"): http://sozd.duma.gov.ru/bill/419090-7.

- **Гарант – Перспективы регулирования финансового рынка: законодательное закрепление цифровых прав, статуса специальных субъектов лизинговой деятельности, правил категоризации инвесторов http://www.garant.ru/news/1238063/**

«Уже в феврале во втором и третьем чтениях может быть принят пакет законопроектов в сфере цифровой экономики: о цифровых финансовых активах, о закреплении в Гражданском кодексе норм о цифровых правах, о привлечении инвестиций с использованием инвестиционных платформ. Об этом сообщил вчера на пресс-конференции председатель Госдумы по финансовому рынку Анатолий Аксаков. Напомним, еще в начале прошлой – осенней – сессии палаты проекты были существенно доработаны: из них, в частности, исключены такие термины, как криптовалюта, токен, майнинг и пр., и предложен общий подход к регулированию отношений, связанных с цифровыми правами и цифровыми финансовыми активами. Сейчас, как подчеркнул депутат, анализируются замечания к скорректированным текстам документов Совета при Президенте РФ по кодификации и совершенствованию гражданского законодательства (далее – совет по кодификации). Стоит отметить, что пока совет по кодификации рассмотрел (29 ноября прошлого года) только новую версию законопроекта о цифровых финансовых активах. Среди основных замечаний к нему: недостаточная определенность в соотношении понятий "цифровые финансовые активы" и "цифровые права" (из содержания проекта можно сделать вывод о том, что цифровые финансовые активы – это совокупность цифровых прав, однако прямо об этом не говорится), отсутствие перечня денежных требований, которые могут быть удостоверены цифровыми правами, необоснованность предложения о введении цифровых прав на доли в уставном капитале ООО, неограниченность перечня эмитентов цифровых прав и активов (что позволит войти в их число и так называемым фирмам-однодневкам) и др. Два других законопроекта совет по

кодификации обсудит 17 января, и, судя по проектам заключений[2], концептуально поддержит, несмотря на ряд замечаний.

Также в приоритете рассмотрение законопроекта о категоризации инвесторов – физических лиц. Для граждан, относящихся к каждой из предлагаемых четырех категорий: особо защищаемый неквалифицированный инвестор, простой неквалифицированный инвестор, простой квалифицированный инвестор, профессиональный квалифицированный инвестор – будет определен перечень доступных финансовых инструментов и сделок. Предполагается, что осуществлять категоризацию инвесторов будут обязаны профессиональные участники рынка ценных бумаг: брокеры, форекс-дилеры, доверительные управляющие и т. д.

Всего, по прогнозам Анатолия Аксакова, в рамках весенней сессии будут рассмотрены около 80% внесенных в Госдуму законопроектов, ответственным комитетом по которым является Комитет Госдумы по финансовому рынку, – на сегодняшний день их 67. Среди них, помимо уже перечисленных, законопроекты о регулировании отношений операторов по переводу денежных средств и поставщиков платежных приложений (типа Google Pay, Apple Pay и т. п.), уточнении требований к деятельности на территории России иностранных платежных систем и иностранных поставщиков платежных услуг, возможности возврата заемщику уплаченной им страховой премии при отказе от договора страхования в связи с досрочным погашением потребительского кредита и др.»

- **Coinspot – Рынок криптовалют в РФ: Спекуляции, большие надежды и крупный теневой сегмент https://coinspot.io/law/russia_sng/rynok-kriptovalyut-v-rf-cpekulyacii-bolshie-nadezhdy-i-krupnyj-tenevoj-segment/**

«Криптовалютная сфера развивается очень быстро. Речь не столько о капитализации рынка (из-за волатильности курса биткоина и альткоинов объём всё время меняется), сколько о признании криптовалют государством, бизнесом, обычными пользователями сети. Ситуация в России несколько отличается от того, что происходит на Западе, включая Европу и США. О том, в чём заключаются эти различия и чего можно ожидать от рынка криптовалют в России, рассказывает исполнительный директор SONM Олег Любимов.

Рынок расчётов непосредственно в криптовалютах, по моему мнению, – наиболее глобальный из всех рынков, для него нет границ национальных государств, поэтому перевод средств соседу не отличается от перевода на другой континент. С учётом этого выделить российский сегмент крипторынка технически сложно. Однако такое разделение имеет смысл для рынка криптобирж и особенно обмена криптовалют на фиатные деньги, так как обмен цифровых валют на валюты, эмитируемые государствами, – это та область крипторынка, которая может регулироваться и потому зависит от локальной законодательной базы.

О ситуации с криптовалютами в России

С моей точки зрения, в России крипторынок сейчас регулируется примерно никак. С одной стороны, криптовалюты в явном виде не запрещены, однако практика такова, что любое юрлицо и тем более финансовая/кредитная организация, которая рискует работать с ними, немедленно попадает под давление со стороны проверяющих/контролирующих

органов, которые намекают, что так делать не надо. Все всё понимают, поэтому легального оборота криптовалют в России по сути нет.

Такое положение имеет серьёзные последствия для отечественного рынка. Доля РФ в легальной части мирового рынка обмена криптовалют составляет, по разным оценкам, от 0% до 0%, и это вовсе не шутка. Проблема в том, что в России нет ни одной легально работающей криптобиржи, единственная крупная и ориентированная в том числе на рынок России/СНГ площадка официально зарегистрирована в Сингапуре. Есть несколько успешных российских блокчейн- и криптопроектов, однако они также официально зарегистрированы за пределами РФ, в более привлекательных для ведения такого рода бизнеса юрисдикциях.

Несмотря на то, что официальных криптобирж и обменников в России нет, теневой сегмент, безусловно, присутствует, представляя собой большую неопределённую величину. Мне известно об огромном количестве примеров обналичивания криптовалют, об их использовании, к примеру, иностранными рабочими для отправки средств на родину. Даже в криминальной хронике всё чаще мелькают сообщения о мошенничестве и других преступлениях, связанных с процедурами купли/продажи криптовалют, что позволяет косвенно сделать выводы о масштабе явления.

Влияние криптовалют на денежно-финансовую систему РФ сейчас и прогноз на ближайшее будущее

Я считаю, весь рынок криптовалют – это один большой вызов денежно-финансовой и непосредственно связанной с ней банковской системе национальных государств. Эмиссия ничем не обеспеченных инфляционных денег – это относительно недавняя монополия государств современного типа, но однозначно ставшая одной из ключевых. Она необходима для поддержания работы всей системы в её нынешнем виде (безусловно выгодном в первую очередь государственным элитам).

Невозможно представить, что кто-то успешно запустит в оборот валюту, не подконтрольную ни одному государству, с предсказуемым механизмом эмиссии, которым нельзя злоупотреблять, и прямыми платежами, минуя банки или платёжные системы-посредники. Хотя постойте-ка….

Если серьёзно, то надо понимать, что биткоин и другие криптовалюты уже с нами и, видимо, навсегда. Точно предсказать изменения, которые повлечёт их появление, трудно, но уже понятно, что они будут значительными, так как слишком очевидны преимущества криптовалют, работающих по заранее заданному алгоритму, прозрачному для всех участников системы (по сравнению с деятельностью центробанков большинства стран мира, соревнующихся в скорости эмиссии произвольных объёмов фиатных денег).

Я часто слышу мнение о том, что появление криптовалют ничего принципиально не изменило в экономике, так как они в основном используются для спекуляций. Однако такая точка зрения не учитывает, что мы находимся на очень ранней стадии проникновения криптовалют. Если сравнивать с развитием интернета, то, условно, это 1980-е, когда интернет уже был, но до появления веба, то есть сайтов в привычном нам понимании, ещё достаточно далеко. Современный криптовалюты мало пригодны для использования неподготовленными пользователями, ими мало где можно расплатиться за реальные товары и услуги, сами платежи медленные и неудобные. Но и интернет 30 лет назад был уделом

небольшого числа энтузиастов, имеющих высокую квалификацию. За следующие 30 лет благодаря интернету изменилось всё.

Законопроект «О цифровых финансовых активах» – что с ним не так?

Российские законопроекты в данной области оставляют тяжёлое впечатление. У меня, например, складывается ощущение, что у авторов, конечно, есть видение того, что они хотят получить в результате, но это видение никак не соотносится с реальностью, в которой мы находимся. Я обсуждал данный законопроект с некоторым количеством специалистов отрасли– даже самые лояльные из них не верят, что этот закон может выполняться в реальности.

Для легализации рынка криптовалют не обязательно придумывать что-то своё, можно использовать опыт других стран: они уже сделали ошибки, которых можно избежать, получили положительный опыт, который необходимо учесть.

О зарубежье

В абсолютном большинстве развитых стран криптовалюты легальны. По всей видимости, действует логика «Если невозможно запретить, то надо возглавить». Однако они пока мало где признаны полноценным платёжным средством/валютой, чаще их относят к активам того или иного типа: нематериальный актив, виртуальный товар, виртуальная ценная бумага, прочие виды активов (не знаю, что у людей в голове и не могу прокомментировать, зачем они это делают вместо того, чтобы называть всё своими именами). Выделяется разумностью в первую очередь Великобритания, которая трактует биткоин как иностранную валюту (чем он, по сути, и является для любого государства), а также Швейцария, которая признаёт его платёжным средством и много делает для развития этой сферы экономики (например, в отдельных кантонах биткоин принимают к оплате местных сборов).

Что касается России, то спрогнозировать развитие криптовалютного рынка сейчас сложно, уж слишком много действует разноплановых факторов. Хотелось бы верить, что общий вектор развития будет направлен в нужную инвесторам и обычным пользователям сторону. Только в этом случае экономика страны получит приятный бонус в виде доходов с хорошо отлаженной криптовалютной сферы. Эксперты считают, что с криптовалютами бороться не стоит, необходимо рациональное регулирование, которое позволит избежать некорректных действий со стороны недобросовестных участников рынка. С этим мнением нельзя не согласиться».

- **РБК – Алексей Моисеев: криптовалюты перестали быть финансовой пирамидой**
  https://www.rbc.ru/crypto/news/5c3f20309a794778413d720a

«Заместитель министра финансов России считает, что блокчейн-индустрия изменилась в положительную сторону

В криптовалютах больше нет признаков финансовых пирамид, об этом на Гайдаровском форуме заявил замминистра финансов России Алексей Моисеев, сообщает News.ru. Он добавил, что анонимность криптовалют и операций в блокчейне – это иллюзия.

«Финансовая пирамида – это элемент (криптовалют, – прим. ред.), о чем я говорил, за что меня неоднократно подвергали остракизму. Но я думаю, что она (финансовая пирамида) была, и сейчас признаков ее, на мой взгляд, нет», – сказал Моисеев.

Ранее ректор РАНХиГС Владимир Мау предположил, что криптовалюта может стать заменой доллару. В то же время премьер-министр России Дмитрий Медведев посоветовал не хоронить цифровые деньги, а продолжать следить за их развитием».

- **Fingramota.org – Регулирование криптовалют в разных странах мира**
  http://www.fingramota.org/lichnye-finansy/investitsii-i-sberezheniya/item/2340-regulirovanie-kriptovalyut-v-raznykh-stranakh-mira

«Стоимость всех криптовалют в мире перевалила за $500 млрд. Согласно сервису, позволяющему следить за капитализацией каждой из существующих цифровых валют CoinMarketCap, сегодня капитализация крипторынка составляет $536,04 млрд, причем на долю биткойна приходится почти 35% всего рынка. Новый платежный инструмент уверенно завоевывает мир – центробанки развитых стран не могут больше игнорировать его распространение и потихоньку начинают искать подходы к регулированию криптовалют.

На текущий момент законодательные нормы, касающиеся обращения цифровых валют, успели установить только несколько стран. Россия в этот список не входит.

Россия

В октябре 2017 года в Кремле прошло совещание по вопросу использования цифровых технологий в финансовой сфере, по итогам которого президент РФ утвердил перечень поручений, охватывающих основные вопросы легализации криптовалют в стране. До 1 июля 2018 года правительство и Центробанк должны будут подготовить все необходимые поправки в законодательство, которые предусматривают определение базовых понятий, касающихся крипторынка, и создать базовый нормативно-правовой акт, регулирующий правовой статус и порядок обращения криптовалют в России.

В конце декабря Министерство финансов и ЦБ представили проект закона «О цифровых финансовых активах», который, в том числе, предлагает решения к регулированию сферы ICO.

В то же время глава Банка России Эльвира Набиуллина неоднократно отмечала, что позиция ведомства по отношению к криптовалютам неизменна: регулятор не поддерживает легализацию цифровых валют в качестве законного платежного средства, но считает лежащую в их основе технологию блокчейн весьма перспективной.

Беларусь

С декабря 2017 года криптовалюты, их добыча и операции в стране официально разрешены. Соответствующий декрет «О развитии цифровой экономики» был подписан президентов БР Александром Лукашенко. Таким образом, Беларусь стала фактически первым в мире государством, который открыл широкие возможности для использования технологии блокчейн.

Согласно декрету, любая деятельность по майнингу, приобретению, отчуждению токенов, осуществляемая физическими лицами, в Беларуси не является

предпринимательской деятельностью, и токены не подлежат декларированию. До 2023 года все это не будет облагаться налогами.

США

Цифровые деньги не признаны официальным платежным средством в США и считаются имуществом (как золото или недвижимость). С 2014 года по отношению к некоторым видам деятельности, связанным с использованием криптовалют, применяются те же требования, что и к имуществу, в отдельных случаях, что и к размещению ценных бумаг и прочие.

С 1 января 2018 года все транзакции с «цифрой» в США облагаются налогом. Поправки, вносящие соответствующие изменения в Налоговый кодекс страны, были ранее подписаны президентом Дональдом Трампом. Если раньше виртуальная валюта рассматривалась как имущество и некоторые операции с ней (например, обмен одной криптовалюты на другую) не облагались налогом, теперь за каждое взаимодействие с «цифрой» американцы будут платить в казну. Если гражданин США будет хранить у себя криптовалюту менее года, ему придется заплатить государству прогрессивный налог в размере от 10 до 37% в зависимости от его личного уровня доходов, более года – налог на долгосрочный рост капитала, ставка которого может доходить до 24%. За обмен одной виртуальной валюты на любую другую также придется заплатить подоходный налог.

Европейский союз

Пока ни один из регулирующих органов Евросоюза не принял каких-либо специальных правил регулирования криптовалютной деятельности. Налогообложение виртуальной валюты и операций с ней осуществляется в соответствии с национальным законодательством государств-членов ЕС в зависимости от природы криптовалютной операции. В большинстве стран оборот «цифры» неподконтролен, а ее продажа не облагается налогом, хотя еще в 2014 году Европейский центробанк рекомендовал банкам не проводить операции с использованием виртуальных валют, пока не будет установлен режим регулирования.

В то же время европейские государства в будущем намерены ужесточать имеющиеся правила для того, чтобы предотвращать отмывание денег и финансирование терроризма посредством криптовалютных платформ. О таком намерении уже заявили в Великобритании. Правительства Германии и Франции уже сотрудничают в целях проведения анализа рисков, связанных с биткойном.

Великобритания

Цифровые деньги в Великобритании рассматриваются в качестве иностранной валюты, биткойн – как «частные деньги». Операции по обмену самой популярной в мире криптовалюты на национальную или иностранную валюты на Туманном Альбионе не облагаются налогом. При этом в установленном порядке взымается сбор при сделках купли или продажи товаров и услуг, осуществляемых в криптовалюте. Доходы, полученные от спекуляций с «цифрой», облагаются налогом на прирост капитала.

В ближайшем будущем Великобритания намерена включить цифровые активы в рамки существующего законодательства относительно отмывания денег и финансирования терроризма.

Швейцария

В этой стране вопрос правового статуса криптовалют остается нерешенным, хотя биткойн уже активно выполняет функции валюты в реальной экономике. Например, национальный железнодорожный оператор продает биткойны в своих кассовых аппаратах, а в кантоне Цуг их принимают в качестве оплаты за коммунальные услуги.

Операции с криптовалютами в Швейцарии не требуют специальных разрешений, но некоторые виды коммерческой деятельности, включающие использование цифровых денег, подлежат лицензированию.

Япония

В Японии цифровые валюты в апреле 2017 года были признаны платежным средством. Для того чтобы разграничить понятие криптовалюты и электронных денег, «цифру» признали не денежным средством, а оборотоспособным активом, который может быть использован в качестве платежного средства.

В стране работает Комиссия по цифровым активам Японии.

Китай

Единый подход к правовому регулированию криптовалютных отношений в Китае еще не выработан, хотя в стране находится один из быстрорастущих финтех-рынков в мире. С сентября минувшего года в стране действует запрет на публичное размещение виртуальной валюты, деятельность криптовалютных бирж запрещена, но все, что касается деятельности физических лиц (хранение, операции с «цифрой»), не регулируется.

В СМИ то и дело появляется информация о том, что Китай планирует запретить добычу виртуальных денег местными компаниями – власти обеспокоены финансовым риском и тем, что майнинг потребует чрезмерного расхода электроэнергии.

Сингапур

В Сингапуре криптовалюты рассматриваются как финансовый актив, а не средство платежа. В некоторых случаях они могут быть классифицированы как ценные бумаги и облагаться соответствующим налогом.

Законодательно статус цифровой валюты детально не урегулирован, но есть правовое регулирование отдельных видов деятельности, связанных с ее обращением.

Как сообщил глава Денежно-кредитного управления Сингапура (MAS) Рави Менон, Центробанк страны не исключает выпуска национальной криптовалюты.

ОАЭ

На сегодняшний день в Объединенных Арабских Эмиратах нет четкой нормативно-правовой базы для компаний и бирж, которые представляют индустрию цифровых валют. Однако в октябре минувшего года правительство Абу-Даби выпустило базовое руководство в отношении криптовалют и их публичного размещения, согласно которому лицензированные компании, которые предоставляют или используют цифровые валюты для финансовых услуг, обязаны придерживаться существующих законов по борьбе с отмыванием денег и финансированием терроризма.

В январе 2018 года Центробанк ОАЭ пошел еще дальше и опубликовал новую нормативно-правовую базу, определив виртуальные валюты как «любой вид цифровой единицы, используемой как средство обмена, создания счета или хранения ценностей» и запретив провайдерам платежных услуг проводить любые транзакции в криптовалютах».

- **CRYPTOR – Регулирование криптовалют в 2018: текущая ситуация в мире**
  https://cryptor.net/regulirovanie-kriptovalyut/regulirovanie-kriptovalyut-v-2018-tekushchaya-situaciya-v-mire

«Если 2017 стал “годом ICO”, то 2018, однозначно, станет “годом законодательной расплаты”. Ситуация уже начала накаляться, так как правительства по всему миру заметили криптовалюты и теперь пытаются понять, как к ним относиться. Одни страны приветствуют крипту, другие пока не определились, а третьи настроены откровенно враждебно. В кратком обзоре мы расскажем о правовом положении криптовалют в 15 странах мира.

США

В США еще не сформировалось единого мнения властей о криптовалюте. Звучат только заявления о намерении правительства “скоро определиться” со своей политикой в отношении криптовалюты.

Комиссия SEC, контролирующая оборот ценных бумаг на бирже, выступила с предостережением о высокой рискованности вложений в криптовалюту, приостановила ряд ICO и потребовала усиления госрегулирования криптосферы.

CFTC, “заведующая” товарными фьючерсами, разрешила проведение сделок с криптовалютными деривативами. Кроме того, CFTC организовала публичные слушания по вопросу изменений правил обращения этих деривативов. Впрочем, одно из заседаний пришлось перенести из-за приостановки работы федерального правительства США.

Министр финансов Стив Мнучин является сторонником фиатных валют и противником крипты. Выступая в Экономическом клубе в Вашингтоне 12 января, Мнучин сообщил, что его ведомство (и ряд других) изучают возможность применения крипты для отмывания незаконных доходов. Кроме того, по его словам, Совет по надзору за финансовой стабильностью США (FSOC) сформировал рабочую группу по изучению крипторынка. Мнучин также хочет наладить работу с “большой двадцаткой” по предотвращению превращения биткоина в аналог “банковского счета в Швейцарии”.

На Всемирном экономическом форуме 25 января Мнучин вновь указал на то, что основной задачей Минфина в отношении криптовалют является “предотвращение их использования в противозаконных целях”.

Замеместитель Мнучина по терроризму и финансовой разведке Сигал Мандельker поддержал своего начальника. Во время своего визита в Токио он приветствовал решения властей Китая, Гонконга и Южной Корее по борьбе с анонимной торговлей криптовалютами. По его словам, аналогичные правила нужно ввести по всему миру.

Также нужно отметить проблемы криптоинвесторов из-за пределов США, вызванные необходимостью соблюдать лицензионные требования каждого отдельного штата. Если власти США будут считать криптовалюты валютой, то решения федерального правительства будут иметь приоритет над решениями штатов. Если же криптовалюты будут

считаться “ценными бумагами” (SEC пока не ответила на этот вопрос однозначно), то крипторынку (и, в особенности, ICO) придется иметь дело с законами каждого штата по отдельности (как это происходит сейчас).

Канада

Агентство по защите прав потребителей финансовых услуг Канады (FCAC) не считает криптовалюты “законным платежным средством” - под это определение попадает только канадский доллар. Однако канадские законы не так суровы, как кажутся на первый взгляд. На самом деле, в вопросах взаимодействия с криптой у этой северной страны, вероятно, самое прозрачное и понятное законодательство в мире (за исключением разве что Швейцарии).

После многих недель слушаний, на которых выступали такие эксперты, как Андреас Антонопулос, канадский парламент в 2014 году принял “Билль С-31” - первый на планете общегосударственный криптовалютный закон. CSA - контролер рынка ценных бумаг Канады - в прошлом году разослал письмо, в котором сообщил, что к криптовалютным сделкам применимы все канадские законы об обороте ценных бумаг.

Стивен Полоз, руководитель Центрального банка Канады, впрочем, не слишком благоволит крипте. С его точки зрения, тот же биткоин не является валютой, а стоимость крипты основана на спекуляции и элементе азартной игры.

Канада также присоединилась к “предостерегающей директиве” NASAA - ассоциации контролеров рынка акций в Северной Америке - в которой говорится о риске мошенничества.

Венесуэла

Эту латиноамериканскую страну нельзя назвать крупной фигурой ни в мировой экономике, ни в криптосфере. Однако политика этой страны в отношении криптовалют заслуживает серьезного внимания. Правительство Николаса Мадуро хочет обойти санкционный режим с помощью обеспеченной нефтью национальной криптовалют - “петро”.

Под властью Мадуро страну уже несколько лет раздирают протесты и столкновения оппозиции с правительством. 2017-й год Венесуэла начала с планов запрета криптовалют, притом что боливар (национальная валюта) из-за инфляции стал почти бесполезным. И даже в декабре 2017 года правительство намеревалось взять под контроль майнинг в стране - глава государственного управления по криптовалютам Карлос Варгос заявил о составлении национального реестра майнеров.

В условиях, когда фиатная валюта почти ничего не стоит, а санкции США усиливаются, введение “петро” может сделать Венесуэлу - несмотря на режим - одной из самых прогрессивных в отношении криптовалют стран (даже если единственной целью будет обеспечение продаж “петро”).

Япония

Законодательство Японии в отношении криптовалют не является либеральным. Сейчас она с трудом выигрывает борьбу за привлечение криптобизнеса, бегущего из Республики Корея и КНР, где правительства или “выдавливают” крипту, или постоянно

меняют свою позицию. Японские власти однозначно лучше относятся к криптовалютам, чем соседи по региону.

Впрочем, недавние события могут охладить японский энтузиазм. Взлом площадки Coincheck, приведший к похищению более 530 миллионов долларов в токенах NEM, спровоцировал расследования со стороны японского контролера финансовых услуг (FSA).

КНР

Китайские власти последовательно “перекрывают кислород” крипторынку. Сперва в здесь запретили проведение ICO, затем из страны начали выдавливать майнеров, заморозили банковские счета, замеченные в активности на крипторынке, и запретили доступ ко всем интернет-ресурсам, посвященным криптовалютной торговле.

Китайское криптовалютное законодательство - наиболее строгое среди всех крупных экономик мира. При этом в 2017 году в Китае работало более половины майнеров мира, а объем торговли криптовалютами между рядовыми пользователями в Китае рос быстрее, чем в любой другой стране мира.

В то же время, суровость китайских криптовалютных законов вполне укладывается в активно ведущуюся правительством Си Цзиньпина политику противодействия коррупции и борьбы с оттоком капитала.

Южная Корея

Еще недавно Южная Корея гордилась своим высоким положением в криптомире, а на фоне китайских запретов прошлого года воспринималась как криптовалютная “страна-убежище”. Однако в начале этого года обнаружился раскол среди южнокорейского руководства по “криптовалютному вопросу”. Он сопровождался целым рядом заявлений, пояснений и публикаций ложной информации. Эта неопределенность и перспектива возможного запрета стала причиной “Красного вторника” - обвала крипторынка 16 января. Аналогичный обвал произошел и 30 января - когда корейские власти начали применять на практике принятый 23 января запрет анонимной торговли криптовалютами.

И, в качестве дополнительного внешнеполитического штриха к разворачивающейся драме раскола правительства, менее чем год назад отправившего в отставку президента, Департамент финансовых услуг (DFS) американского штата Нью-Йорк запросил у 6 южнокорейских банков, имеющих филиалы в Нью-Йорке, данные о счетах, связанных с криптовалютной торговой деятельностью.

Сингапур

Регулирование криптовалют в Сингапуре выглядит очень прогрессивным, особенно на фоне соседей по азиатско-тихоокеанскому региону. Сингапурский Центробанк (MAS) на пике “взлета” биткоина в конце прошлого года выпустил предупреждение о спекулятивных рисках на крипторынке. Сингапурский международный коммерческий суд тогда же провел заседание по спору о криптовалютной сделке, тем самым “узаконив” активы, бывшие предметом спора.

Сингапурский вице-премьер в январе этого года заявил, что законы его страны не различают транзакции фиатных и цифровых валют.

Руководитель отдела финтеха MAS 24 января сообщил, что битку не грозит скорая финансовая катастрофа, подобная истории с банком Lehman Brothers (банкротство этого банка стало “спусковым механизмом” острой фазы экономического кризиса 2008 года). Он добавил, что “регуляторы начинают воспринимать криптовалютный рынок всерьез”. Также по его словам, регуляторам нужно будет применить механизмы защиты потребителя к цифровым валютам вроде биткоина, чтобы рынок продолжил рост.

В то же время от MAS пока не было официальных заявлений по поводу взлома японской биржи Coincheck, в результате которого было похищено 530 миллионов долларов в криптовалюте. Целью атаки была сингапурская монета NEM.

Индия

Индия когда-то воспринималась как благодатная среда для криптовалют, однако в 2018 году правительство начало откровенно “душить” крипту. Объяснения запретов у индийских властей вполне привычные: опасность отмывания доходов, облегчение финансирования терроризма, налоговые махинации, обеспечение нелегальной деятельности и тому подобное. При этом в Индии до сих пор в основном используют наличные деньги.

Местные представители криптоиндустрии, впрочем, убеждены, что власти не потянут воплощение в жизнь запрета “в китайском варианте”.

Австралия

После финансового скандала вокруг главного банка страны, власти Австралии планируют использовать японский опыт в сфере крипторегулирования и противодействия отмыванию доходов. Эта позиция отличается от той, которую власти занимали в 2015 году - тогда правительство решило не вмешиваться в жизнь криптомира. Однако отсутствие четких “правил игры” оказало скорее негативное влияние: в конце 2017 года криптоброкеры были вынуждены приостановить прием австралийских долларов из-за “нежелания банков сотрудничать” с криптоиндустрией.

В декабре 2017 Австралийское налоговое управление выпустило рекомендацию, из которой можно понять направленность будущих правил работы с криптовалютой в стране:

“Транзакции в сети биткоина сходны с бартерными сделками, со сходными налоговыми последствиями. С нашей точки зрения, биткоин не является деньгами или иностранной валютой и поставка биткоина не является финансовой поставкой с точки зрения налога на товары и услуги, но является активом с точки зрения налога на прирост капитала”.

Некоторые австралийские политики выступают в поддержку криптовалют. Так, в августе прошлого года сенаторы от обеих основных партий (лейбористской и консервативной) призвали Резервный банк Австралии начать прием криптовалюты в качестве официальных платежных средств. Так что будущее крипты в “стране антиподов” пока неясно, но оно вполне может быть благоприятным.

Великобритания / Евросоюз

Хотя Брекзит и должен привести к выходу Соединенного Королевства из ЕС через год, их планы в отношении крипты остаются сходными. В декабре The Guardian и The

Telegraph написали, что британское Казначейство и ЕС намерены положить конец анонимной криптоторговле, оправдываясь борьбой с отмыванием доходов и уклонением от уплаты налогов.

Евросоюз намерен потребовать от криптовалютных платформ проводить полноценную юридическую экспертизу всех клиентов, а также сообщать контролирующим органам обо всех подозрительных транзакциях. Аналогично, британское Казначейство заявило, что из-за “опасений, связанных с использованием криптовалют, будет стараться привести криптовалютные биржи и кошельки в соответствии с законодательством по отмыванию денег”. Казначейство, впрочем, признало, что “существует мало свидетельств использования криптовалют для отмывания денег, но риск этого растет”.

Несмотря на заявления еврокомиссара по экономике и финансовым делам Пьера Московиси, что ЕС не собирается регулировать биткоин, заявление комиссара противоречит другим сообщениям. Так, спустя всего два дня вице-президент Еврокомиссии Валдис Домбровскис заявил репортерам в Брюсселе:

“Существуют явные риски для инвесторов и потребителей, связанные с высокой волатильностью, включая риск полной потери инвестиций, операционные проблем, взлома, рыночных манипуляций и неисполнения обязательств”.

Призывы к ужесточению контроля за криптовалютами в Европе озвучивали и в январе. Так, министр экономики Франции Брюно Ле Мэр заявил о создании специальной рабочей группы цифровым валютам. Член правления немецкого Бундесбанка Иоахим Вюрмелинг также призвал к контролю криптовалют на общемировом уровне.

Домбровскис в конце января подтвердил свою позицию по криптовалютам, написав сразу трем надзорным органам Европы, предупреждая о “пузыре” биткоина. 25 января “в бой” вступила премьер Великобритании Тереза Мэй, повторившая утверждения заявления главы МВФ Кристин Лагард и президента США Дональда Трампа. В интервью Bloomberg на Всемирном экономическом форуме в Давосе премьер-министр заявила:

“Мы должны очень серьезно следить за ними (криптовалютами - ред.) из-за того, как они могут быть использованы, в особенности преступниками”.

Ожидается, что правила работы с криптой Евросоюз и Великобритания озвучат этой весной.

Швейцария

Уважение к правам личности в банковском деле, которым славится Швейцария, распространилось и на криптосферу. Швейцария не входит в ЕС и благосклонно воспринимает цифровые деньги.

Министр экономики страны уже заявил о своем желании сделать Швейцарию “криптонацией”. Госсекретарь минфина, в свою очередь, заверил Financial Times, что власти хотят процветания рынка ICO, но он должен будет соответствовать швейцарским финансовым стандартам.

Также в Швейцарии была создана группа, разрабатывающая правила проведения ICO с задачей “обеспечить правовую определенность, честность финансового центра и

технологически-нейтральное регулирование". Она будет отчитываться перед Федеральным советом Швейцарии в конце этого года.

Россия

Власти России, как и правительство Южной Кореи, еще не разобрались, что им делать с криптовалютой. В сентябре 2017 года Банк России не планировал считать крипту платежным инструментом или воспринимать ее как зарубежную валюту. То есть российские власти рассматривали прогрессивный принцип невмешательства государства в крипторынок.

Однако в том же сентябре замглавы минфина Алексей Моисеев заявил, что оплата чего-либо криптой "на данный момент незаконна". После чего он добавил, что из-за существующего правового вакуума не может сказать, легальны ли криптовалюты в целом или нет.

До этих заявлений, министерство финансов РФ считало, что работать с криптовалютами должны иметь право только "квалифицированные инвесторы". Президент Путин поддержал минфин, приведя обычный набор аргументов про отмывание нелегальных доходов, неуплату налогов, денежное обеспечение терроризма и обилие мошенников.

Минфин подтвердил свою жесткую позицию по крипте 28 декабря, предложив ввести налогообложение для майнеров. Признаков скорых правовых сложностей для криптовалют в России в новом году стало только больше, так как Путин 11 января вновь поддержал минфин, отметив, что в будущем может понадобиться законодательное регулирование криптовалютного рынка.

Через две недели был опубликован законопроект минфина "О цифровых финансовых активах". Если он будет принят, то даст юридические определения токенам, утвердит правила ICO и майнинга.

Кандидат в президенты Борис Титов 26 января назвал предложенный законопроект слишком суровым. Исходя из заявления пресс-службы Титова, "Минфин предлагает значительно более строгое регулирование, чем Япония, Швейцария, Беларусь и Армения; то есть все страны, принявшие соответствующие законы. Лучше бездействовать, чем принять такой закон".

Еще больше неопределенности вносит озвученное замминистра финансов Моисеевым опасение, что принятый в Беларуси в декабре "Декрет о развитии цифровой экономики" может привести к оттоку капитала из России в Беларусь, если РФ примет жесткие законы в отношении крипты.

Нигерия

Крупнейшая экономика Африки недавно пострадала от рецессии, которая вызвала острую нехватку фиатной валюты. Оборот биткоина в Нигерии за прошлый год вырос на 1500% - нигерийцы использовали крипту, чтобы обойти ограничения на доступ к американскому доллару, введенные для того, чтобы сдержать рецессию. И если в начале года нигерийский центробанк намеревался запретить криптовалюты, то к концу уже утверждал, что не может контролировать биткоин и блокчейн, так как он им не принадлежит.

Хотя в декабре МВФ сообщил, что Нигерия вышла из рецессии, скромные прогнозы по росту ВВП и опора на экспорт сырой нефти делают призывы главы нигерийского Центробанка Годвин Эмфиле к взятию крипты под контроль довольно сдержанными. Он ограничивается сравнением битка с азартными играми, но не призывает к запрету.

Гана

В Гане биткоин и, тем более, вся остальная крипта, не считается законным платежным средством. Несмотря на то что парламент Ганы рассматривает законопроект, разрешающий работу с криптовалютами (вероятнее всего, посредством компаний, получивших от правительства лицензию “издателя цифровых денег”), на сегодняшний день Гана, согласно Graphic Online, является “одной из шести стран, объявивших биткоин вне закона”.

Кроме того, Group Ndoum - крупнейший инвестиционный банк Ганы - рекомендовал Центробанку вложить 1 процент резервных средств в биткоин.

ЮАР

Позиция ЮАР по криптовалютам - одна из наиболее прогрессивных в мире. В 2014 Резервный Банк ЮАР опубликовал документ, разъясняющий его позицию по криптовалютам, который был весьма благожелателен к отрасли. В июле 2017 года правительство Южной Африки начало совместную работу с компанией Bankymoon - местным поставщиком услуг блокчейна - над “сбалансированным” подхода к регулированию крипты.

ЮАР уже сталкивалась с проблемами девальвации своей фиатной валюты, южноафриканского рэнда. В 2015 рэнд упал на 26 процентов из-за снижения курса китайского юаня всего на 2 процента. В 2017 ЮАР вновь столкнулась с девальвацией рэнда после того, как президент отправил в отставку главу минфина. В 2018 году власти ЮАР еще не говорили о криптовалютах, так что отразится ли южноафриканская опора на Китай в их позиции по криптовалютам, пока неизвестно».