РИСКИ ПРИМЕНЕНИЯ ФИНАНСОВЫХ ТЕХНОЛОГИЙ И СОЗДАНИЕ УСЛОВИЙ ДЛЯ ИХ СНИЖЕНИЯ

Андрей Лисицын,
к.ю.н., советник председателя Правления НП «НПС»

Финансовые технологии (финтех) в большинстве случаев, особенно в обращениях к конечным потребителям (не в профессиональной среде), позиционируются как абсолютное благо. И действительно, ведь очевидная цель финтех-проектов – удобство (включая снижение цены, упрощение доступа к услуге и т.п.), а также безопасность осуществления финансовых операций. Разве это не благо? Несомненно, благо, но…

Вот об этом «но» и пойдет речь в данной статье, и не потому, что автор негативно относится к развитию финансовых технологий. Как раз наоборот, автор убежден, что применение финансовых технологий будет иметь устойчивое, ди-

намичное (а не, мягко говоря, ажиотажное) развитие на среднесрочном и долгосрочном горизонтах только при условии осознанного восприятия этого явления не только профессионалами и провайдерами соответствующих услуг, но и конечным потребителем. Ведь, если провести аналогию с транспортом, люди когда-то очень боялись поездов, а сегодня это самый безопасный транспорт, в свою очередь, по статистике несчастных случаев, автотранспорт остается самым опасным, но количество использующих его только растет. Пользователи автотранспорта, естественно, давно уже осознают все риски, но удобство заставляет принять их, требуя создания системы снижения этих рисков. Следовательно, задача тех, кто отвечает за развитие технологий, состоит не только в демонстрации всех преимуществ новый технологии, но и в создании условия для осознания рисков, связанных с применением финансовых технологий, взвешивания этих рисков относительно преимуществ применения соответствующих технологий.

На практике в настоящее время о преимуществах финансовых технологий говорится крайне много, а вот риски их применения, к сожалению, обсуждаются урывками и с большой неохотой. Например, пользователю, да и всем, обязательно расскажут: как быстро растет курс какой-нибудь криптовалюты (цифровой валюты); как удобно (а прежде всего дешево) с ней осуществлять операции, как безопасны операции с этими «валютами» (если только, конечно, она функционирует на другой крайне популярной и сильно популяризируемой технологии – блокчейн); не забудут коснуться анонимности (ведь «кому-то», к сожалению, это тоже крайне важно). Будут описывать множество других преимуществ, оставляя за рамками анализа (видимо, как несущественное по сравнению с преимуществами) такие аспекты, как возможность взлома (изъяны информационной безопасности), отсутствие юридических гарантий при осуществлении операций с цифровыми валютами, высокую волатильность этих «активов» и много еще чего, гораздо менее очевидного.

Цифровые валюты здесь приведены в качестве наглядного и очень громко звучащего в последнее время примера, но дело обстоит не лучше в уже ставших более привычными и, что самое главное, массовыми, а в некоторых случаях даже обязательными финансовыми технологиями. Возьмем, к примеру, банковские карты. Стремясь развить, по сути, государственную систему платежных карт, в России обязали выдавать карты национальной системы платежных карт (карты МИР) всем получателям выплат из бюджета. Расширение использования национальных платежных инструментов можно только приветствовать, но вот почему-то в связи с таким расширением не обсуждается и, соответственно, не решается вопрос с рисками, которые возникают в связи с такой массовой «окартизацией» населения. Причем речь может идти не столько о рисках использования таких инновационных и попрежнему актуальных финансовых технологий, как платежные карты, а с рисками, которые возникают, даже если операции с использованием полученной карты ни разу не осуществлялись. На практике выдача платежной карты многими кредитными организациями (включая крупнейшие) сопровождается фактически автоматическим предоставлением этому клиенту доступа к другой

финансовой технологии – к онлайн-банку (системе дистанционного банковского обслуживания), в котором можно увидеть и приобрести практически все продукты этого банка, в том числе вклады, никак не связанные с использованием платежных карт. И, вероятно, многим это удобно, однако ни они, ни те, кому онлайн-банк совсем не нужен (например, большинство пенсионеров), не уведомляются и часто даже не подозревают о том, что через канал онлайн-банка злоумышленники, например, методами психологического воздействия на владельца карты и одновременно «счастливого» владельца доступа в онлайн-банк (методами т.н. «социальной инженерии») могут получить возможность осуществить списание не только денег на счете по карте, но и средств на его вкладах, по-прежнему никак не связанных с использованием платежных карт.

Несомненно, онлайн-банк является удобным как для клиента, так и для банка способом коммуникаций. Клиент получает практически круглосуточный сервис, а банк – удобный канал продаж, повышающий скорость оборота денежных средств клиента и его осведомленность о продуктах банка. Но почему при этом не происходит прямого и явного раскрытия рисков привязывания к удаленным каналам счетов и вкладов, которые клиент стремится использовать как инструмент сбережения, а не как средство обращения? Почему клиент зачастую не имеет возможность также просто, как включился онлайн-банк, отключить его или исключить из него отдельные продукты (например, вклады)? Все это вопросы риторические.

Уже проведенное беглое описание ситуации с внедрением финансовых технологий показывает, что на государственном уровне, в профессиональной среде необходима отдельная дискуссия не только о преимуществах финансовых технологий, но и о связанных с их внедрением и развитием рисках, способах управления этими рисками. Таким образом, целью настоящей статьи является создание определенной основы для такой дискуссии путем формулирования и характеристики системы рисков использования различных финансовых технологий на самом массовом, розничном сегменте рынка. Эта попытка систематизации может лечь в основу для дальнейшей дискуссии о целесообразности развития и широкого внедрения тех или иных финансовых технологий, для глубокого и продуманного соотнесения удобства их применения и иных преимуществ с рисками их использования.

Под рисками принято понимать вероятность возникновения негативных последствий от чего-либо при определенных обстоятельствах, следовательно, для целей настоящей статьи под рисками применения финансовых технологий предлагается понимать любую вероятность наступления неблагоприятных последствий для пользователей, провайдеров финансовых услуг и для экономики в целом, связанную с применением финансовых технологий при определенных обстоятельствах и в определенных ситуациях. Соответственно, риски применения финансовых технологий можно разделить на клиентские риски (риски пользователя), риски провайдера, риски системные (риски экономики и общества в целом). В настоящей статье для начала дискуссии предлагается остановиться на системе клиентских рисков применения финансовых технологий и на определении условий по управлению этими рисками.

Риски пользователей финансовых услуг, связанные с применением финансовых технологий, можно разделить на две большие группы:

прямые риски – вероятность наступления негативных последствий непосредственно для пользователя, применяющего финансовую технологию;

косвенные риски – вероятность наступления неблагоприятных последствий для пользователей, связанных с нарушением стабильности системы в целом, ухудшением качества жизни и общественной безопасности. Эти риски на первый взгляд не наносят прямого ущерба пользователям, однако их реализация в конечном счете влияет на каждого пользователя, хотя бы потому, что снижает удобство использования технологий и увеличивает стоимость соответствующих услуг из-за мер, применяемых для управления такими рисками.

В настоящей статье для начала дискуссии предлагается остановиться на системе клиентских рисков применения финансовых технологий и на определении условий по управлению этими рисками.

СРЕДИ ПРЯМЫХ РИСКОВ МОЖНО ВЫДЕЛИТЬ СЛЕДУЮЩИЕ ОСНОВНЫЕ ВИДЫ:

1) **Риск кражи значимых данных –** вероятность наступления негативных последствий для пользователя финансовых технологий в связи с кражей не самого актива, а ключей доступа к управлению этим активом.

Удаленность доступа к услуге, с одной стороны, является удобством, с другой – связана с отсутствием личного контакта пользователя и провайдера, что делает для последнего трудно различимым, а часто вообще не различимым то, кто конкретно осуществляет операцию – пользователь или мошенник.

Достаточно обсуждаемым примером реализации данного риска является кража данных платежных карт, осуществляемая методами фишинга (пользователь сам передает достаточную для осуществления операции платежную информацию или эта информация перехватывается программными средствами, например вирусами) или скимминга (данные, позволяющие сделать дубликат карты, копируются программно-техническими средствами) и позволяющая осуществлять операции со средствами пользователя от его имени, но без его ведома и участия.

Другой (уже описанный выше) пример связан с получением злоумышленниками доступа к системам онлайн-банка средствами психологического воздействия на пользователя, так называемыми методами «социальной

инженерии». Отличительной особенностью этих методов является то, что пользователь понимает, что отдает данные, но считает, что делает это для своей выгоды.

Оба перечисленных выше примера касаются кражи данных, необходимых для осуществления списания денежных средств. В случае выявления такой кражи пострадавший может просто заблокировать соответствующий инструмент и начать пользоваться другим (правда, и здесь с онлайн-банками не все так просто). Более существенные по своим последствиям случаи имеют место при краже персональных данных, особенно тех, которые используются для идентификации личности при осуществлении удаленных операций.

Например, в настоящее время в России активно обсуждается вопрос о создании централизованной системы биометрической идентификации, предполагающей сбор и хранение биометрической информации, используемой для удаленной идентификации и аутентификации личности. Проблема состоит в том, что в случае хищения или подмены такой информации лицу будет крайне сложно доказать, что действие осуществлял не он или даже что он – это он, т.е. может произойти «кража личности». В этом случае устранение последствий кражи персональных данных сильно затруднено по сравнению с ликвидацией последствий кражи платежных данных, поскольку получить новые биометрические данные, если не невозможно, то крайне трудоемко.

Указанные риски использования биометрической идентификации усугубляются в том случае, если хранение и использование такой информации осуществляются на централизованной основе и соответствующие базы являются доступными для потенциально неограниченного круга лиц.

Именно такая централизация и использование баз предлагается в настоящее время в России при обсуждении соответствующего законопроекта о биометрической идентификации. Представляется, что в связи с этим законопроектом требуется дополнительный анализ описанных рисков, а также выработка предложений по созданию системы управления ими и использованию альтернативных каналов предоставления соответствующих услуг по удаленной идентификации.

2) **Рыночные риски –** вероятность наступления негативных последствий (чаще всего – прямых убытков) от существенного изменения рыночной ситуации (стоимости какого-то актива, величины ставок, динамично изменяющихся условий сделки и т.п.).

Этот вид риска связан не столько с самим применением технологий для осуществления финансовых операций, сколько с вложением средств в финансовые технологии, которые, по сути, являются разновидностью соинвестирования (ICO, карудсорсинг, краудфандинг и т.п.). Вместе с тем расширение применения финансовых технологий для соинвестирования существенно повышает риски осуществления соответствующей деятельности, поскольку связано с еще большей виртуализацией объекта вложений и, следовательно, со сложностью оценки этого объекта. Например, большинство проектов соинвестирования на базе обращения криптовалют делают упор не на ценность самого объекта инвестирования, а на увеличение цены инвестиций за счет его номинирования «в быстро растущей» (на самом

деле – сильно волатильной) цифровой валюте. В результате речь идет не столько об инвестиции, сколько о спекуляции, т.е. о совсем другой системе рисков и способах управления ими.

3) **Риск нарушения бесперебойности предоставления услуги –** вероятность наступления неблагоприятных последствий в связи с невозможностью использования привычной финансовой технологии, прежде всего из-за технологических сбоев или ошибок в архитектуре самого сервиса или каналов его предоставления.

Логичным следствием применения любых удаленных сервисов является выработка у клиента привычки их использования. Следовательно, в случае неожиданного прекращения возможности осуществления операции с применением привычной технологии для клиента неизбежно наступают негативные последствия, в том числе материального характера. Например, если клиент всегда осуществлял погашение очередного платежа по кредиту с использованием каналов дистанционного банковского обслуживания, неожиданное перекрытие этого канала с высокой вероятностью приведет к просрочке. Банк, конечно, может сказать, что есть офисы, но клиент, правомерно рассчитывавший на удаленный канал, может быть на момент осуществления очередного платежа далеко от этих офисов. А перекладывание на клиента юридическими приемами ответственности за просрочку в указанной ситуации не меняет сути проблемы и вряд ли способствует развитию финансовых технологий и формированию в России цифровой экономики.

4) **Риски в сфере защиты прав и законных интересов пользователей –** вероятность наступления неблагоприятных последствий в связи с невозможностью или с существенным затруднением защиты прав пользователей услуг, предоставляемых с использованием финансовых технологий.

Эти риски обусловлены преимущественно удаленным характером предоставления услуг, с использование финансовых технологий. В результате соответствующие услуги на территории России могут фактически оказываться лицами, находящимися за пределами юрисдикции Российской Федерации, в том числе функционирующими в рамках регулирования офшорных юрисдикций. Следовательно, применение российских механизмов защиты прав и интересов пользователей становится практически невозможным.

5) **Риски введения в заблуждение пользователя относительно провайдера услуг** (включая риск анонимности провайдера услуг) – вероятность наступления неблагоприятных последствий в связи с невозможностью или с существенным затруднением определения провайдера, отвечающего за качество предоставления услуги с использованием финансовых технологий.

При применении финансовых технологий с пользователем зачастую непосредственно контактирует финтех-компания, однако формально услуга предоставляется другим лицом, обладающим соответствующей лицензией или разрешением на осуществление деятельности (лицензированный провайдер). Так нередко происходит при осуществлении платежей в Интернете (платежные агрегаторы) или при оказании услуг финансового посредничества (предоставления возможности осуществления операций на финансовых рынках, вклю-

чая внебиржевые операции с производными финансовыми инструментами).

Визуально (а иногда и документально) пользователю демонстрируется, что ему предоставляются услуги лицензированного провайдера (оформление сайта, предоставление подтверждающих документов в электронном виде и т.п.), хотя фактически услугу предоставляет финтех-компания. В результате в случае возникновения сбоев и прямых нарушений прав и законных интересов пользователю крайне трудно разобраться и (или) предъявить претензию к кому-то и получить соответствующее возмещение. Финтех-компания юридически не оказывает эти услуги, а лицензированный провайдер всячески старается юридическими конструкциями перенести риски пользования такими услугами на самого пользователя. Такая ситуация также не способствует развитию финансовых технологий и формированию в России цифровой экономики.

Таким образом, состав прямых рисков, связанных с применением финансовых технологий, достаточно широк. Однако карта рисков будет совсем не полной без перечисления видов косвенных рисков применения финансовых технологий.

Пользователю зачастую трудно понять, обращается он к услугам российской или иностранной компании. В результате под действием механизмов недобросовестной конкуренции увеличивается стоимость услуг национальных провайдеров.

СРЕДИ КОСВЕННЫХ РИСКОВ ПРИМЕНЕНИЯ ФИНАНСОВЫХ ТЕХНОЛОГИЙ МОЖНО ВЫДЕЛИТЬ:

1) **Риск применения финансовых технологий для целей отмывания доходов, полученных преступным путем, и финансирования терроризма –** вероятность наступления негативных последствий в связи с криминализацией финансового сектора, которая может привести не только к ухудшению качества услуг, но и к полной потере средств добросовестных пользователей соответствующих услуг.

Ключевыми факторами для реализации данного риска являются:

- возможность обеспечения анонимности осуществления операций с использованием финансовых технологий;
- возможность технологического обеспечения бесконечности и обрыва цепочки посредников, при осуществлении операции (например, автоматизированное дробление с последующей агрегацией сумм), существенно затрудняющей выявление конечных выгодоприобретателей операций и, соответственно, расследование преступлений.

2) **Риски регуляторного арбитража** – вероятность наступления негативных последствий в связи с осуществлением деятельности на территории России провайдерами, требования к деятельности которых в государстве их инкорпорации существенно слабее требований, установленных в России. В конечном итоге это приводит к возникновению описанных выше прямых рисков (риски в сфере защиты прав и законных интересов пользователей, риски введения в заблуждение пользователя относительно провайдера услуг), а также к ухудшению качества соответствующих услуг в связи с действием механизмов недобросовестной конкуренции.

Развитие финансовых технологий и прежде всего удаленных каналов оказания услуг является ключевым фактором данного риска. Пользователю зачастую трудно понять, обращается он к услугам российской или иностранной компании. В результате под действием механизмов недобросовестной конкуренции увеличивается стоимость услуг национальных провайдеров (им надо как-то компенсировать регуляторные и иные издержки) и (или) снижается качество услуг иностранных.

3) **Риски стресоустойчивости технологий** – вероятность наступления негативных последствий в связи с невозможностью получения услуг в случае неожиданного возникновения длительных технологических и (или) организационно-правовых препятствий (например, санкций) для их оказания в условиях отсутствия альтернативных каналов обслуживания, находящихся в «горячем резерве».

Особенно существенные последствия возникают при реализации данных рисков в платежной индустрии, поскольку влекут кризис неплатежей и, соответственно, препятствуют реализации практически всех экономических отношений.

Например, если гипотетически все перейдут на использование платежей с использованием телефона, то в случае централизованной блокировки всех телефонов (большинство из которых иностранного производства) или каналов связи при отсутствии иных платежных средств может возникнуть невозможность осуществления розничных платежей в принципе. Эта ситуация приведена скорее для иллюстрации, и пока сложно себе представить ее воплощение, но такой же риск, уже гораздо менее гипотетический в условиях текущей геополитической напряженности, может иметь место и повлечь существенные последствия в случае блокировки использования Интернета, через который работают практически все современные системы осуществления расчетов. В этом случае даже снять наличные в банкоматах будет невозможно.

Описав, таким образом, один из возможных подходов к анализу системы рисков применения финансовых технологий, в заключение представляется целесообразным остановиться на мерах, которые могут быть применены для снижения этих рисков.

ПРЕДСТАВЛЯЕТСЯ, ЧТО СУЩЕСТВЕННОМУ СОКРАЩЕНИЮ УКАЗАННЫХ РИСКОВ БУДЕТ СПОСОБСТВОВАТЬ ОСУЩЕСТВЛЕНИЕ СЛЕДУЮЩИХ МЕРОПРИЯТИЙ:

1) Недопущение возникновения правового вакуума. Все финансовые технологии, которые могут быть использо-

ваны российским пользователем, должны подпадать под какую-то систему правового регулирования. Причем запреты возможны только после внедрения механизмов выявления и пресечения недобросовестных и противоправных практик.

Для обеспечения реализации этого механизма представляется целесообразным создание с привлечением экспертного сообщества межведомственной комиссии (с участием представителей Банка России, Минфина России, Росфинмониторинга, Минэкономразвития, Минкомсвязи, ФСБ, ФСТЭК, МВД), обладающей в соответствии с законодательством правом отнесения к той или иной системе российского регулирования конкретных технологий и сервисов, а также правом ограничения применения к этим технологиям и сервисам отдельных требований российского законодательства в пределах строго ограниченного времени и в рамках четко определенных параметров, осуществления соответствующей деятельности, в том числе в части отчетности соответствующих провайдеров (механизм «регуляторных песочниц»).

Кроме создания организационно-правовой основы для выявления и управления описанными выше рисками без длительного и зачастую запоздалого внесения законодательных изменений, такая система позволит активно и легально внедрять новые технологии.

2) Обеспечение прозрачности сервисов – установление требований, что любые сервисы, доступные с территории России, привлекающие денежные средства, имущество или обрабатывающие данные клиентов (данные платежных карт, персональные данные), должны размещать на своих ресурсах в сети Интернет определенную информацию, в частности: о порядке оказания услуг, о провайдере, о юридических основаниях оказания соответствующих услуг, о субъектах рассмотрения претензий пользователей и т.п. Соответственно, ресурсы провайдеров, не выполняющих такие требования, должны рассматриваться как фишингвые и блокироваться на уровне разделегирования доменных имен (т.е. фактически запрета использования соответствующего интернет-домена). Соответствующая практика разделигирования уже активно нарабатывается Банком России, однако ее расширение требует установления указанных законодательных требований.

3) Внедрение, в том числе на законодательном уровне, механизмов предотвращения навязывания применения удаленных сервисов, например, путем установления требования об эквивалентной сложности подключения и отключения соответствующих сервисов. Не должно быть ситуаций, когда сервис подключается автоматически (нажатием одной кнопки), а отключается, например, только личной явкой в центральный офис провайдера.

4) Создание системы выявления в России недобросовестных практик в сфере применения финансовых технологий на основе обратной связи с пользователями любых удаленных сервисов. Функционирование такой системы не должно зависеть от юридического статуса провайдера и государства его инкорпорации, иначе останутся лазейки для регуляторного арбитража и (или) для реализации описанных выше рисков введения в заблуждение пользователя относительно провайдера услуг. RF