Актуальные вопросы кибербезопасности и повышения финансовой грамотности в эпоху цифровых технологий

М. А. Ефремов, К. М. Казаманова, А. В. Ширяева
Финансовый университет при Правительстве Российской Федерации (Финуниверситет), Financial University
efremov_mikle@mail.ru

***Аннотация*. Финансовые махинации с гражданами – это наиболее распространенная проблема современного российского общества. Большая часть населения России сталкивалась с ними хотя бы раз в жизни и мало кто смог противостоять этому. В данной статье рассмотрены основные виды финансовых махинаций, способы борьбы с ними, а также предложили свои варианты повышения финансовой грамотности населения с целью защиты его от противоправных действий и улучшения их благосостояния.**

Ключевые слова: кибербезопасность; фишинг; финансовые махинации; цифровые технологии; финансовые пирамиды; фарминг

Развитие цифровых финансовых технологий открывает большие перспективы для расширения доступа к финансовым услугам и повышения финансовой грамотности населения и, как следствие, благотворно влияет на благосостояние всех категорий граждан. Тем не менее, разносторонний потенциал цифровых финансов пока не до конца очевиден как потребителям, так и финансовым институтам. Со стороны потребителей существует психологический барьер. Большое количество людей, прежде всего из социально уязвимых слоев населения, избегают новых финансовых инструментов, опасаясь потерять те сбережения, которые у них есть, или попросту не доверяя неосязаемым услуге или продукту. Другими словами, их тревожит недостаток или полное отсутствие человеческого контакта при выборе и оформлении финансовой услуги. Кроме того, потребители не всегда понимают и верно воспринимают маркетинговые сообщения и методы, используемые финансовыми учреждениями в продвижении новых продуктов. Ситуация также усугубляется еще новыми рисками для потребителей стать жертвами кибермошенничества или утечки личных данных, что также отрицательно сказывается на уровне их доверия к цифровым финансовым продуктам.

Что касается финансовых институтов, то основным источником проблемы является резко повысившийся уровень конкуренции на финансовом рынке, который заставляет многих сосредоточиться на наиболее прибыльных направлениях деятельности, на фоне чего теряется интерес к клиентам со средним и низким уровнями дохода. Кроме того, продвижение цифровых финансовых услуг часто не охватывает их возможности для этой категории потребителей. Наконец, не все финансовые институты считают необходимым уделять достаточно внимания созданию дружественных потребителю интерфейсов онлайн продуктов и услуг.

Развитие цифровых финансовых услуг будет способствовать расширению географического охвата финансовых услуг; обеспечению прозрачность финансовых потоков; снижению стоимости финансовых услуг; созданию новых, высококачественных финансовых продуктов, отвечающим потребностям различных групп потребителей, включая категории населения с ограниченным доступом к финансовым услугам; увеличению возможностей для информирования и консультирования потребителей финансовых услуг посредством телекоммуникационных каналов, онлайн платформ и автоматических сервисов.

Финансовым институтам совместно с регулятором предстоит адаптировать отраслевые стандарты ответственного финансового поведения с целью минимизации рисков для потребителей, связанных с переходом на цифровые финансовые продукты и услуги. В центре внимания – решение проблемы кибербезопасности, которое потребует комплексного подхода и постоянного взаимодействия всех участников финансового рынка.

Финансовое мошенничество касается каждого. Поэтому следует рассматривать данную проблему максимально честно и просто. Согласно результатам общероссийского опроса, проведенного ГК «ЛИК ПРО», 80% респондентов хотя бы раз в 2016 году становились жертвами мошенников. С высокой долей вероятности можно утверждать, что каждому приходили сообщения от «наших детей» с целью вымогания денег. Зачастую граждане становятся участниками ожесточённой битвы против никому ненужных, навязанных платных услуг. Но это только незначительная доля всего спектра финансовых махинаций, в которые пытаются вовлечь каждого. Действительно, схем по отмыванию кровно заработанных денег существует достаточно много. И если одни еще можно распознать, имея лишь здравый смысл в своем арсенале, то для защиты от других требуются определённые знания в финансовой и правовой сферах. В данной статье рассмотрены наиболее часто встречающиеся

из них, а также предложены методы увеличения уровня финансовой грамотности населения.

Итак, к наиболее распространенным видам мошенничества можно отнести: звонки и смс-сообщения с просьбой перевести деньги на определённый номер телефона; спам с предложением легко и быстро заработать много денег; финансовые пирамиды; фишинг; фарминг; скандинавский аукцион.

Рассмотрим первый вид мошенничества. Для её распознавания достаточно использовать простую цепочку действий. Если вдруг Ваш ребенок попал в нелегкую ситуацию и ему срочно нужны деньги, всегда можно перезвонить, даже если он слезно умоляет в своем сообщении этого не делать. Еще одним простым, но достаточно эффективным способом будет проверка номера мобильного телефона в сети Интернет. достаточно просто набрать его в поисковой строке.

Во втором виде мошенничества также не представляется сложным для вычисления. Для того чтобы не попасться в эту ловушку достаточно запомнить несколько простых правил.

Во-первых, Вам никто и никогда не будет предлагать денег просто так. Во-вторых, высокая доходность и маленький риск – это две совершенно несовместимые вещи. Нормальной доходностью считается 3-4% в год, не больше. Больше (6-7%) – это уже высокая доходность, которая может быть и не является приманкой для легковерных граждан, ибо и такая доходность может быть от инвестиционных проектов, но тут риск уже становится выше. А вот такие доходности как 15%, 20% или больше, как минимум, должны заставить задуматься.

Третий вид мошенничества – финансовые пирамиды. Они появились еще в средневековой Европе, и даже в России за столь непродолжительную историю рыночной экономики было немало скандалов с подобными пирамидами. Стоит вспомнить общеизвестную историю с инвесторами и билетами МММ, ООО «Русский Дом Селенга» или «Хопер Инвест», когда люди выстаивали многочасовые очереди, чтобы сделать самый «выгодный вклад в своей жизни».

С развитием интернет-технологий проблема построения финансовых пирамид приобрела поистине глобальный характер, и мошенники разных уровней и компетенций стали использовать более изощренные формы обмана инвесторов, чем вышеперечисленные. Чтобы не попасть в хитрые сети мошенников, достаточно соблюдать несколько несложных правил:

1) Все сообщения или звонки, которые приходят вам на телефон, нужно проверять на предмет информации в интернете. Номер телефона можно попробовать ввести в поисковой системе. Если этот номер уже фигурировал в какой-то схеме, то наверняка вы найдете жалобы людей.

2) Если конкурс заявлен как сайт какой-то известной организации, то стоит поискать в интернете на их портале информацию об этом либо номер телефона и позвонить по горячей линии. Так вы сможете подтвердить или опровергнуть информацию. Если вам говорят, что у вас есть час на совершение какого-то действия, значит, вас наверняка обманывают. Звонить вам будут в этом случае с городского номера, а не с мобильного.

Все схемы мошенничества, основанные на принципах пирамиды, в соответствии с присущей им структурой построения можно **разделить на три группы**. Некоторые создатели заверяют, что сумели создать качественно новую схему. Однако при тщательном анализе любую из них можно отнести к одной из представленных ниже групп (табл. 1).

ТАБЛИЦА I ГРУППЫ СХЕМ ФИНАНСОВЫХ МОШЕННИЧЕСТВ, ОСНОВАННЫХ НА ФИНАНСОВОЙ ПИРАМИДЕ

Признак для сравнения	**Одноуровневая пирамида**	**Многоуровневая пирамида**	**Матричная пирамида**
Структура	В центре находится владелец проекта. Вклады поступают к нему до определенного момента, именно он распределяет вознаграждения.	Несколько участников. Организатор пирамиды взаимодействует только с первым уровнем, но курирует деятельность всей пирамиды.	Центральным звеном являются несколько активных участников. Новичками они интересуются, пока те приводят новых вкладчиков.
Источник образования прибыли	Инвестиционные, а также благотворительные проекты.	Исключительно вступительные взносы новых участников. Структура пирамиды может маскироваться продажами различных продуктов.	Только взносы вступающих вкладчиков. Чтобы пустить пыль в глаза, используются усложненные схемы продажи какого-либо товара.
Срок действия	Зависит исключительно от возможностей убеждать, которые присущи организатору.	Крах наступает очень быстро, так как пирамида разрастается ускоренными темпами.	Может быть довольно длительным, потому что точные сроки заполнения матриц неизвестны.

Примером интернет пирамиды можно назвать «Кэшбери».[1] ЦБ РФ назвал холдинг «Кэшбери» крупнейшей в России финансовой пирамидой, в которую были вовлечены тысячи россиян. «Кэшбери» — финансовая организация, привлекающая деньги под обещание гигантских процентов и выдающая микрозаймы. И до сообщения из Центробанка о ней писали в основном

лишь восторженные отзывы. Medialeaks рассказывает, как компания создаёт себе успешный образ в интернете и почему для клиентов всё может быть не так радужно.

На официальном сайте «Кэшбери» называет себя «площадкой, сводящей инвесторов и заёмщиков». Компания привлекает деньги инвесторов, обещая выгодный процент. На сайте заявлена доходность до 265 процентов годовых. Также «Кэшбери» предлагает вкладывать деньги в её криптовалюту, обещая в этом случае 550 процентов годовых. Ещё на сайте выдают займы под 1,2 – 2,2 процента в день. Прибыль от этих микрозаймов и обещают инвесторам. Помимо этого, говорится о всевозможных бонусах и премиях тем, кто приведёт с собой новых клиентов. В социальных сетях вокруг «Кэшбери» создаётся положительный образ. Можно найти десятки постов от клиентов, которые уверяют, что с помощью этой компании заработали хорошие деньги. Правда, при прочтении некоторых постов начинают закрадываться сомнения, что их пишут люди. Признаками финансового мошенничества являются: отсутствие лицензии у организации на осуществление экономической деятельности; обещание вкладчиком высокой доходности; настаивание на том, что высокая финансовая доходность обусловлена новыми сверхприбыльными методами инвестирования; призыв быстрее вкладывать деньги, не раздумывая; выплаты клиентам из вкладов других клиентов; отсутствие информации о рисках; отсутствие по договору выплат вкладчикам в случае разорения компании; утаивание реквизитов компании; обязательное подписание расписки о неразглашении конфиденциальной информации; необходим сбор при осуществлении клиентами вклада и зависимость размера их прибыли от количества привлеченных ими других клиентов. Как мы можем видеть «Кэшбери» соответствует некоторым критериям финансовой пирамиды. И привлечение организаторов к ответственности было лишь вопросом времени.

Сегодня жизнь любого человека невозможно представить без сотен тысяч килобайт информации, которые он получает и отправляет через сеть Интернет. Однако именно Всемирная паутина в настоящее время является пристанищем разного рода мошенников, которые готовы присвоить средства любого доверчивого пользователя.

Четвертый вид мошенничества – фишинг. Это одна из наиболее распространённых схем похищения платёжных реквизитов и паролей пользователей компьютеров. Как часто пользователи присматриваются к адресу, который введён в адресной строке? Можно предположить, что чаще всего не присматриваются. Из этого следует, что любой сайт, оформленный по аналогии с сайтом банка или сайтом платёжного кошелька, не вызовет у пользователя никакого недоверия. Источник фишинговых угроз таится в малоизвестных интернет-магазинах, а также спам-ссылках в социальных сетях и на интернет-почте, т.е. на тех интернет-страницах, которые предполагают введение конфиденциальной информации. Основная задача мошенников – отвлечь внимание человека, представив на экране страницу, полностью идентичную странице платёжной системы, которой он пользуется. В отдельных случаях фишинговый сайт предполагает взаимодействие с реальными людьми. Так, известен случай, когда клиент одного из банков, после того как вошёл в копию своего онлайн-кабинета, ввёл номер сотового телефона и имел продолжительную беседу с неким «работником банка». Тот предлагал клиенту сообщить некоторые личные данные, включая пин-код банковской карты.

Как уберечься от фишинга?

Рецепты есть, и они достаточно просты: 1) перед тем как ввести платёжные реквизиты и пароль, необходимо обратить внимание на начало адресной строки. Поскольку передача сведений происходит по защищённым каналам, в начале адресной строки должны находиться буквы «http://.» 2) важно внимательно изучить адрес сайта в адресной строке. Ни в коем случае нельзя вводить личные данные на странице сайта, в адресной строке которого изменена хотя бы одна буква 3) пользователь должен остерегаться перехода по непроверенным рассылкам со взломанных страниц 4) нужно использовать только проверенные страницы интернет-магазинов. Опасность малоизвестных интернет-магазинов в том, что они не только обманут клиентов с платёжной системой, но и просто не вышлют заказанный товар. В результате клиенты лишатся и денег, и покупки.

Модернизированной версией фишинга является фарминг. Пользователя посредством заражения компьютера вредоносными программами направляют на сторонние сайты для последующего списания денежных средств или получения информации. Характерным видом фарминга является заражение компьютера вирусной программой с целью майнинга – зарабатывания криптовалюты путём незаконного использования чужих производственных мощностей. Заражение происходит независимо от желания человека при посещении самых различных сайтов, поэтому действенным вариантом защиты является качественная антивирусная программа, блокирующая вирус в момент заражения.

Достаточно популярным способом незаконного обогащения за чужой счёт является скандинавский аукцион. Можно ли аукцион считать мошенничеством? Конечно, нет, однако сама схема очень благоприятствует использованию её и в преступных целях. Модель выманивания денег достаточно проста. На аукцион выставляется товар с первоначальной стоимостью всего в один рубль. Шаг аукциона составляет 0,25 у.е., однако за право сделать такой шаг участник должен уплатить на порядок больше, предположим, 100 у.е. Таким образом, за то, чтобы увеличить первоначальную цену необходимо будет каждую вновь сделанную ставку оплачивать дважды – шагом самой ставки и комиссией в 100 у.е. После завершения аукциона товар продаётся участнику, предложившему последнюю ставку. Обман кроется не только в двойной цене аукциона, ставки после которого возвращаются проигравшим его, но комиссия остаётся у аукциониста. Активными участниками подобного рода аукционов являются роботы, чья цель – не дать закончиться игре до тех пор, пока владелец товара не

получит требуемый доход. Зачастую, роботы могут выигрывать аукционы все аукционы, на последней секунде повышая ставку.

Как же защититься от финансового мошенничества? Во-первых, нужно повышать финансовую грамотность. Во-вторых, существует возможность прибегнуть к помощи финансового омбудсмена.

Общественный примиритель на финансовом рынке (финансовый омбудсмен) – орган внесудебного рассмотрения споров, возникающих между финансовыми организациями и их клиентами – физическими лицами. [2] Это независимое лицо, защищающее интересы граждан, у которых возникли проблемы с финучреждениями. Процедура рассмотрения спора омбудсменом бесплатная, к тому же разрешение конфликта происходит во внесудебном порядке, что позволяет быстро улаживать разногласия между клиентом и финансовой организацией. Прибегать к такому способу разбирательства стоит в том случае, если стоимость спора невелика. Впервые пост омбудсмена был введен в Германии в 1992 году Союзом немецких банков (VdB). На сегодняшний день ее примеру последовали многие страны мира – Великобритания, Франция, Дания, Швеция, Италия, Норвегия, Португалия, Польша, ЮАР и т.д. [3]

В России такой институт появился в 2010 году. Инициатором его создания выступила Ассоциация российских банков (АРБ). 20 сентября 2010 года советом АРБ были утверждены «Положение об Общественном примирителе на финансовом рынке (Финансовом омбудсмене)» и «Регламент Общественного примирителя на финансовом рынке (Финансового омбудсмена)». А в 2018 году Президент РФ, Владимир Путин подписал Федеральный закон от 04.06.2018 № 123-ФЗ "Об уполномоченном по правам потребителей финансовых услуг", в котором прописаны статус, цели деятельности, полномочия финансового уполномоченного и порядок рассмотрения обращения финансовым уполномоченным. Финансовый уполномоченный имеет право решать споры, возникающие между финансовыми организациями и их клиентами, на сумму до 500 тыс. рублей. Инициировать обращение к омбудсмену может только физическое лицо.

Разумеется, омбудсмен не в состоянии полностью избавить заемщика от необходимости выплачивать обременительный кредит. Не станет он защищать и заведомых мошенников. Но зато он может выступить грамотным посредником в уже возникшем споре банка и гражданина, разобрать финансовую претензию, смягчить негативные последствия для обеих сторон с помощью примирительного соглашения. Так, за два года работы первого российского финансового омбудсмена было принято несколько тысяч обращений граждан, жалующихся на банки. Более половины жалоб были удовлетворены, значительная часть – удовлетворена частично. По оценкам экспертов, положительного результата при обращении к финансовому омбудсмену удается добиться почти в 80% случаев.

Наши предложения по контролю финансового мошенничества и повышения финансовой грамотности населения: 1) первое, что можно сделать – это начать бороться с финансовой безграмотностью уже в школе и на 1 год ввести в школах предмет или кружок финансовой грамотности 2) для более взрослого населения можно организовать различные тренинги по фин. грамотности. Можно бесплатные онлайн курсы. Можно включать повышение фин. грамотности в повышение квалификации. Можно обязать консультантов и, осуществляющие финансовое консультирование, организации проводить профилактические беседы/консультирование для повышения финансовой грамотности населения (хотя бы основные аспекты) 3) необходимо изменить менталитет: не бояться привлекать полицию, чтобы решить вопрос с мошенничеством в реальной жизни. Также, необходимо создавать социальную рекламу 4) создать реестр, в который будут занесены личные удостоверения должностных лиц и создать сервис, позволяющий гражданам быстро проверить подлинность стоящего перед ним 5) усовершенствовать ОС в соц. сетях и поисковиках для проверки спама и автопроверки ссылок 6) опять же в интернете: часто реклама, которая привлекает пользователей, заражает вирусами это нужно проверять и ограничивать, либо разработать средство защиты пользователей (блок рекламы или программа пред проверки ссылки).

В заключение необходимо отметить, что финансовое мошенничество до сих пор остается одной из главных проблем современности, несмотря на то, что обо всех схемах уже давно и много раз говорилось. Людям все равно не всегда удается их распознать в силу своей безграмотности. Именно поэтому предложенные нами решения данной проблемы являются наиболее эффективными, так как они смогут предупредить развитие финансовых махинаций.

Список литературы

[1] Басов В. «Звёзды, бабки и образ успеха. Что такое «Кэшбери», которую Центробанк назвал крупнейшей финансовой пирамидой» [Электронный ресурс],URL:https://medialeaks.ru/2609bva-chto-takoe-cashbery/ (дата обращения 28.03.2019)

[2] Звягин Л.С. Современные проблемы динамики социально-экономических систем в фокусе производственных отношений и управляющего развития // Теоретическая экономика. 2018. № 4 (46). С. 76-81.

[3] Звягин Л.С. Комплексная оценка безопасности функционирования моделей экономических систем // Экономика и управление: проблемы, решения. 2017. Т. 4. № 1. С. 18-25.

[4] Звягин Л.С. Системы распределенного моделирования и методы управления модельным временем // Экономика и управление: проблемы, решения. 2018. Т. 1. № 10. С. 4-11.

[5] Федеральный закон от 04.06.2018 N 123-ФЗ "Об уполномоченном по правам потребителей финансовых услуг"Финансовый омбудсмен [Электронный ресурс], URL:https://finombudsman.ru/ (дата обращения 28.03.2019)

[6] Словарь финансовых терминов- Финансовый омбудсмен [Электронный ресурс], URL:http://www.banki.ru/wikibank/finansovyiy_ombudsmen/ (дата обращения 28.03.2019)

[7] Статистика: 80 % Россиян когда-либо становились жертвами мошенников // ЛикPRO Издательский дом Панорама наука и Практика // [Электронный ресурс] URL http://panor.ru/news/statistika-80-rossiyan-kogda-libo-stanovilis-zhertvami-moshennikov.html (Дата обращения 28.03.2019)