

### **3. Основы финансовой безопасности**

Наша финансовая безопасность напрямую зависит от принимаемых нами ежедневно решений. Непродуманный выбор поставщика финансовых услуг, невнимательное чтение условия договоров, отсутствие финансовой дисциплины и - как следствие - неисполнение своих обязательств и неприятная финансовая ситуация.

Развитие технологий затрагивает все сферы нашей жизни. Одним из важнейших современных мега трендов является цифровизация многих процессов, в том числе, финансовых. Значимость цифровых технологий и направления их реализации нашли отражение в программном документе «Цифровая экономика Российской Федерации». Мы ощущаем цифровизацию как жизнь онлайн, мультиэкранность.

Элементы цифровизации:

Диджитализация – перевод содержания бизнес-процессов в цифровой формат

Облачные технологии – электронное хранилище данных в сети Интернет

Интернет вещей – сеть физических объектов со встроенной электроникой, способной общаться с другими объектами. Например: «умный дом», чайник, управляемый со смартфона и т.д.

Искусственный интеллект – свойство интеллектуальных систем выполнять творческие функции

Большие данные (Big Data) – агрегированные данные, предварительно подготовленные для их эффективной обработки

Виртуальная реальность – созданный техническими средствами мир, передаваемый человеку через его ощущения

Дополненная реальность - результат введения в поле зрения сенсорных данных с целью дополнения сведений об окружении и улучшения.

Можно привести целый ряд примеров, показывающих, что цифровая экономика действительно окружает нас и проникает в нашу повседневную жизнь гораздо сильнее, чем кажется на первый взгляд. Цифровые технологии сокращают время коммуникаций, ускоряют все бизнес-процессы, поэтому слабым звеном в современных технологиях все чаще становится человеческий фактор. Цифровые технологии, с одной стороны, приводят к появлению новых возможностей, повышает комфорт для потребителя. С другой, – мы видим, что в один клик сегодня можно потерять свои финансы – количество мошеннических схем, связанных с дистанционными банковскими сервисами, к сожалению, растет.

Сначала о новых возможностях, которые создает цифра.

Основные преимущества цифровых технологий при совершении финансовых операций:

- Упрощение финансовых операций, повышение роли электронных и цифровых денег

- Упрощение платежей
- Сокращение затрат
- Удобство доступа
- Гибкость продуктов
- Быстрое информирование клиента
- Возможность получить отчет и проанализировать операции
- Развитие возможностей дистанционной работы
- Внедрение электронного документооборота
- Более открытый и доступный финансовый рынок
- Повышение финансовой грамотности

Этот список можно продолжить.

В условиях цифровой экономики традиционные финансовые услуги реализуются с помощью цифрового взаимодействия – дистанционная работа с банками, страховыми компаниями, сервисами оплаты налогов, штрафов, коммунальных услуг – появляются новые финансовые услуги в цифровой среде.

В настоящее время широкое распространение получил интернет-банкинг для управления банковской картой. Сейчас многие банки предоставляют эту услугу своим клиентам. Более того, есть банки, которые полностью ушли в интернет и все операции совершаются там. Для управления банковским счетом через интернет-банкинг потребуется лишь компьютер с интернетом и телефон, на который приходят СМС с кодами для подтверждения операций. Это удобно, комиссия, как правило, ниже, чем через отделение банка. При этом вам не только доступен широкий круг операций со своими денежными средствами (переложить деньги со своей зарплатной карты на сберегательный счет, купить иностранную валюту, открыть вклад и так далее), но и есть дополнительные удобные опции - например, история ваших операций (здесь можно проверить, оплатили ли вы счета за ЖКУ за прошлый месяц или запамятали), статистика и анализ расходов, финансовое планирование и прогноз расходов (надо отложить на выплаты по образовательному кредиту, на подарок родным или на поездку на море), настройка автоматических платежей (за коммунальные услуги, телефон или в счет погашения кредита) и многое другое.

Из множества современных инструментов цифровых технологий отметим лишь несколько.

**СМС-банкинг.** Можно управлять услугами и средствами на карте при помощи СМС, которые вы отправляете на специальный номер с определенными командами. Таким способом можно переводить деньги на счет другому физическому лицу (другу или родственнику, репетитору за урок и так далее), пополнять счет, делать перевод через систему денежных переводов и так далее.

**Приложения мобильного сервиса.** Современные банки предлагают своим клиентам собственные приложения мобильного сервиса, которые можно установить на смартфоне или планшете, к которому подключена сим-карта с номером, привязанным к банковской карте. Подключить услугу можно в любом отделении вашего банка, часто бесплатно. Обратите внимание, что в случае управления счетом через мобильное приложение команды отдаются не через сотовую связь, как в случае с СМС-банкингом, а через интернет. Так что если у вас закончился пакет интернета, то купить дополнительный пакет через мобильное приложение вы не сможете, а вот через СМС - вполне. В путешествиях вдали от цивилизации, где сеть буквально приходится ловить, мобильное приложение тоже не поможет, а эсэмэску отправить так или иначе получится.

В мире активно развивается рынок цифровых продуктов для управления личными финансами: сервисы p2p-кредитования, краудлендинга, другие. Например, разработан сервис, который при помощи высокотехнологичного скринга вычисляет, каковы шансы пользователя на получение того или иного кредитного продукта и в каком банке ему точно не откажут в займе

Чаще всего мы пользуемся инструментами цифровой экономики при управлении движением безналичных денег.

Безналичные деньги – это запись на счету в банковской системе, гарант – коммерческий банк. Какими способами управления движением безналичных денег мы пользуемся в настоящее время?

- Можно традиционно обратиться в **отделение** соответствующей **организации** (банка, системы денежных переводов, почты, салона связи и других). Требует затрат

времени, можно обратиться только в рабочее время. В то же время возможен прямой контакт в сотруднике организации, что позволяет задать дополнительные вопросы.

- **Платежный терминал банка.** Работает круглосуточно. Желательно пользоваться терминалами, которые стоят в банковских отделениях - так вы меньше рискуете стать жертвой мошенников.

- **Карта:**

банковская карта, обеспечивающая доступ к банковскому счету владельца;  
• карта, выпущенная по вашему желанию к электронному кошельку и обеспечивающая доступ к некому субсчету в электронной платежной системе;

• карта, дающая вам доступ к рублям или бонусам, баллам, минутам и прочим единицам дополнительной валюты, которые записаны на некоем субсчете в электронной платежной системе, - *платежная карта*.

- **Интернет:**

• *Интернет-банкинг* для управления банковской картой

• *Система Быстрых Платежей*. С начала 2019 года пользователям интернет-банкинга доступен новый сервис Банка России – СБП или Система Быстрых Платежей. Как подсказывает нам название, сервис обеспечивает быстрый перевод денег. В отличие от привычного межбанковского перевода, который занимает несколько часов, перевод через СБП можно назвать мгновенным – деньги поступают на счет получателю в течение нескольких секунд. Кроме того, сервис работает круглосуточно и каждый день, что означает, что деньги можно отправить ночью, а также в выходные и праздничные дни, когда банки не работают. Оператором СБП является Банк России, операционным платежным клиринговым центром – Национальная система платежных карт (НСПК). На официальном сайте сервиса СБП можно найти ответы на частые вопросы – размер комиссии, что делать если деньги не дошли до получателя, отмена перевода и т.д

• *Электронный кошелек* - это средство управления электронными денежными средствами в сети интернет, знакомое многим. По сути, электронный кошелек представляет собой специальную программу или интернет-сервис, который выглядит аналогично личному кабинету в интернет-банкинге. В случае с электронным кошельком вы управляете электронными денежными средствами, которые хранятся на тех самых невидимых пользователю субсчетах электронной платежной системы. Преимущества – защита средств на вашей карте от мошенников, удобство оплаты в интернете

Еще одной сферой цифровизации финансовых услуг является электронная продажа страховых полисов. Это приблизило страхование к потребителю и вывело его на более современный уровень, соответствующий передовым тенденциям развития финансового рынка. Предполагается, что внедрение ИТ-технологий в среднесрочной перспективе приведет к уменьшению расходов страховых организаций на продажи и сопровождение договоров страхования, в том числе урегулирование убытков, что, в свою очередь, должно положительно сказаться как на финансовой стабильности страховщиков, так и на стоимости страховых услуг для потребителя.

Страховщики также начали запускать мобильные приложения, которые уже делают получение страховых услуг более доступным и удобным.

Необходимо отметить наличие важных для населения государственных электронных ресурсов для осуществления платежей. С использованием специальных государственных электронных ресурсов заплатить налоги, оплатить услуги ЖКХ, штрафы может быть не только удобно, но и выгодно.

Онлайн-платежи по оплате налогов, госпошлины, штрафов ГИБДД:

- зарегистрируйтесь на официальном портале [www.nalog.ru](http://www.nalog.ru)или [www.gosuslugi.ru](http://www.gosuslugi.ru);
- вы можете подавать заявку на получение ряда услуг, получать уведомления, заполнять необходимые документы и оплачивать налоги, штрафы, услуги;

– можно воспользоваться возможностью получить скидку на оплату госпошлины, штрафов.

Полезной может быть информация официального портала gosuslugi.ru об оплате госпошлины со скидкой 30%. Скидка действует при электронной подаче заявления и безналичной оплате: банковская карта, электронный кошелек или мобильный телефон. С 1 января 2016 года действует скидка 50% на оплату штрафов ГИБДД. Скидка действует в течение 20 дней со дня вынесения постановления о наложении административного штрафа.

По данным НАФИ (Национальное агентство финансовых исследований) цифровой потребитель финансовых услуг характеризуется следующими чертами поведения, которые позволяют сэкономить время (да и деньги):

19% - не посещают офис, решают все вопросы удаленно (онлайн)

31% - посещают офис реже одного раза в месяц

67% - используют интернет и мобильный банк

11% - используют бесконтактную оплату

3% - используют «умные часы» и браслеты.

Цифровизация финансовых сервисов способствует финансово грамотному поведению. Среди представителей компаний финансового сектора в этом уверены абсолютное большинство. Под влиянием «цифры» финансовая грамотность обрела вполне осозаемое определение наличия у людей конкретного набора устойчивых навыков, помогающих самостоятельно осуществить поиск, оценку и выбор финансовой услуги с целью повышения качества жизни. Это означает, что пользователи финансовых услуг становятся более информированными, ответственными и избирательными в своих финансовых решениях.

Мы видим, что цифровые инструменты обеспечивают быстроту, надежность движения безналичных денег, позволяют экономить наше время на совершение операций. Но интуиция и опыт нам подсказывают, что эти и другие инструменты подвержены рискам. Что такое риск, и какие новые риски несет нам цифровая среда?

Риск – это наличие вероятности незапланированных потерь или доходов. Риск – это отклонения от ожидаемых результатов. Риски могут быть связаны с положительными явлениями, но чаще ассоциируются с потерями, убытками. Любые действия в финансовой сфере подвержены риску. Любая операция, направленная на получение дохода, может закончиться потерями. Приобретая валюту, вы можете как выиграть, так и проиграть на изменении валютного курса. Вкладывая деньги в надежный банк, вы рискуете получить через некоторое время обесценившуюся вследствие инфляции сумму. Факторов риска в финансовой сфере очень много. Соответственно, можно выделить и различные виды рисков. Специфические риски, обусловленные цифровизацией, представлены на слайде.

- риск киберугроз, связанный с проблемой защиты персональных данных (Смартфоны становятся основным средством доступа к цифровым сервисам: ими чаще пользуются для использования электронных финансов, и люди считают, что пользоваться ими легче, чем компьютерами. При этом уровень защищенности этих гаджетов ниже, чем у ПК.);

- «цифровое рабство» – использование данных о человеке для управления его поведением;

- «цифровой разрыв» – разрыв в цифровом образовании, в условиях доступа к цифровым услугам и продуктам, и, как следствие, разрыв в уровне благосостояния людей; недостаточная прозрачность цен и условий;

- сложность подачи жалоб. Например, дистанционное банковское обслуживание, дистанционное заключение договора ОСАГО – это благо или нет? Вроде бы благо: не надо тратить время на то, чтобы стоять в очередях, подписывать бумаги, не требуется физическая досягаемость контрагента. Но это только с одной стороны. А с другой стороны – люди не понимают, какой договор они заключают, с кем и в какой

момент, и где оригинал для спорного случая, и как подтверждать исполнение договора, если вся документация существует в электронном виде. А если ваши персональные данные украли, заключили договор от вашего имени, как доказать, что это не ваши действия?);

- риски нерационального поведения на финансовом рынке как следствие доступности операций для неквалифицированных потребителей финансовых услуг;

- риски подверженности новым инструментам мошенничества с использованием цифровых технологий.

Наверное, можно найти еще целый ряд факторов и видов рисков в цифровой среде. Весьма вероятно, с развитием технологий появятся новые виды рисков. Казалось бы, безопаснее отказаться от любых операций в «цифре», чтобы не подвергать себя такому количеству рисков. Но отказ от современных технологий создает еще один вид риска, последствия и потери которого могут быть тяжелее, чем все то, что мы можем потерять в связи с рисками «цифры». Это риск упущенной выгоды! Представьте, ничего не приобретаем и не оплачиваем в интернете, не пользуемся банкоматами, банковскими картами. К каким дополнительным потерям времени и денег это приведет! И если факторы риска «цифры» могут быть устранины или уменьшены, то риск упущенной выгоды наступает с вероятностью, очень близкой к 100%.

Что делать? Повышать свою цифровую и финансовую грамотность.

**Финансовое мошенничество** — совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.

Рассмотрим несколько видов мошенничества:

- Мошенничества с использованием банковских карт
- Интернет-мошенничества
- Мобильные мошенничества
- Финансовые пирамиды

**Банковская карта.** Удобный инструмент повседневных расчетов.

Самая частая цель атаки мошенников – это безналичные деньги и банковская карта

Согласно обзору мошеннических финансовых операций в России (за период сентябрь 2017 – август 2018), выпущенном Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России (ФинЦЕРТ), в 2017 году мошенникам удалось похитить у населения более 1 млрд рублей.

Банки активно совершенствуют системы безопасности, применяют усиленные системы идентификации клиентов, блокируют подозрительные операции. Сама банковская карта также довольно хорошо защищена от подделок: подобрать наугад нужную комбинацию номера карты, даты действия и CVV-кода достаточно сложно. Таким образом, изготовить поддельную пластиковую карту с параметрами, совпадающими в точности с действительной банковской картой какого-нибудь Скворцова, практически нереально. Соответственно, мошенникам приходится придумывать способы, чтобы каким-то образом списать деньги с вашей карты, не зная ее реквизитов, либо получить все ее реквизиты обманным путем с участием владельца или же украсть реквизиты карты или саму карту без непосредственного участия владельца. Таким образом, можно классифицировать способы финансового мошенничества по этому признаку на три группы:

- Мошенники не знают реквизиты банковской карты. Владелец карты сам совершает действия по переводу средств со своей карты на счет мошенников.

- Мошенники получают обманным путем реквизиты банковской карты. Кража с карты с помощью технических средств (скимминг). Фишиング. Претекстинг (социальная инженерия).

- Мошенники крадут данные / карту без участия владельца. Кража данных с серверов реальных интернет-магазинов. Через недобросовестных сотрудников банка. Кража пластиковой карты.

Способы обмана людей и кражи денег с их банковских карт разнообразны: от подглядывания из-за плеча во время операций с банкоматом и последующего хищения карты до хакерских атак на программное обеспечение.

Основные приемы, которые используют злоумышленники:

- Скимминг или установка специальных устройств на банкоматы (накладная клавиатура, устройство для считывания карт), с помощью которых преступники получают информацию о карте.
- Траппинг - установка на банкомат устройства, которое блокирует карту и не выдает ее обратно, а «добрый» прохожий, якобы пытающийся помочь, подглядывает пин-код и после вашего ухода, забирает карту из банкомата и снимает с нее деньги.
- Магазинные мошенничества, когда во время оплаты покупки или услуги данные карты могут быть считаны и зафиксированы ручным скиммером.
- Фишиング - рассылка электронных писем, в которых от имени банка сообщается об изменениях, производимых в системе его безопасности. При этом пользователей просят возобновить информацию о карте, в том числе указать номер кредитки и ее ПИН-код.
- Мошенничество с помощью телефона - когда клиенту поступают звонки с просьбой погасить задолженность по кредиту, который клиент не брал, и в ходе разговора уточняются данные карты. По похожей схеме может звонить «автоответчик» и собирать необходимые для мошенничества данные.

Во избежание вероятности хищения средств с вашей карты соблюдайте следующие правила:

- При использовании банкомата внимательно осмотрите поверхность над ПИН-клавиатурой и устройство для приема карты на предмет нахождения посторонних прикрепленных предметов.
- Закрывайте рукой клавиатуру при вводе ПИН-кода
- Не передавайте банковскую карту посторонним: ее реквизиты могут быть использованы для чужих покупок.
- Требуйте проведения операций с картой только в личном присутствии, не позволяя уносить карту из поля зрения
  - Никому никогда не сообщайте ваш пин-код или код из смс-сообщения
  - Помните: Банки и платежные системы никогда не прсылают писем и не звонят на телефоны своих клиентов с просьбой предоставить им данные счетов.
- Сообщайте банку актуальные контактные данные
- Подключите услугу SMS- уведомлений, всегда имейте при себе телефон круглосуточной службы поддержки владельцев карт банка - обеспечите эффективную профилактику риска несанкционированных операций по ней.
- Храните ПИН-код отдельно от карты и не пишите его на карте, не сообщайте никому. При его потере или краже немедленно заблокируйте карту

Уберегите себя также и от неприятных последствий собственной невнимательности:

- Своевременно оплачивайте кредит и не превышайте лимит кредитования – это обеспечит отличную кредитную историю и убережет от штрафов
- Не теряйте карту - перевыпуск может стоить дополнительных средств.
- Не снимайте с карты деньги полностью – оставьте некоторую сумму для оплаты комиссий или автоматических платежей.
- В случае смены места работы обратитесь в банк и уточните актуальные для вас тарифы
- При использовании карты за рубежом, помните о курсовой разнице во избежание нежелательного «технического овердрафта».

Перечисленные правила довольно просты и широко известны. Тем не менее многие люди, зная о них, называют данные своей банковской карты, CVV-код, пароли из смс-подтверждений. Почему это происходит? Дело в том, что мошенники применяют приемы социальной инженерии (претекстинг), чтобы вывести человека из состояния спокойного рассудочного мышления.

#### **Приемы социальной инженерии**

1. Предъявляется «приманка», формирующая положительные (выигрыш в лотерее, оплата выставленного вами на продажу товара), или негативные эмоции (претензия по неоплаченному налогу, взыскание по долгам коллекторским агентством, несанкционированное списание средств со счета, блокировка карты).
2. Злоумышленник представляется сотрудником государственных органов, банка, страховой компании, электронного магазина и т.д.
3. Создается дефицит времени для принятия решения: «чтобы приз не ушел к другому, перезвонить или сообщить свои данные нужно в ближайшие пять минут», «чтобы избежать повестки суда, необходимо оплатить задолженность в течение 24 часов» и т.д.

В результате в условиях необходимости быстрого реагирования мозг человека автоматически переводится в состояние стресса и становится более подверженным манипулированию. В этом случае рекомендуется:

1) осознать, что вас ставят в условия немедленного принятия решений, и рассматривать это как сигнал опасности дальнейшего контакта. Покупки-продажи финансовых продуктов и услуг не должны совершаться в течение ближайших 5 минут;

2) необходимо любыми способами убрать дефицит времени, взять паузу, чтобы успокоиться и оценить ситуацию. Можно сказать собеседнику, например, «Мне сейчас неудобно говорить, давайте я вам перезвоню через 20 минут» и, не вступая в дальнейшие переговоры, положить трубку. Человек может говорить вам: «Сейчас или никогда!», и тут смотри пункт первый;

3) проверить информацию, которую вы успели получить от звонившего (например, про двойную аутентификацию, или позвонить по официальному номеру в компанию, которая якобы проводит розыгрыш призов); позвонить родным, другу, кому-то, кто мог бы посмотреть на ситуацию взглядом, не замутненным эмоциями, и указать вам на риск мошенничества.

**Мошенничество в интернете.** Включает в себя все существующие виды обмана, придуманные человечеством за всю историю его существования. Наиболее часто нас могут поджидать неприятности в следующих случаях:

- Покупки через интернет (особенно по предоплате и неоправданно низкой цене)

- При составлении «бесплатного» гороскопа
- При получении смс от якобы платежных систем. На самом деле часто вас поджидает вирус, задача которого - собрать данные о ваших аккаунтах в платежных системах, данные банковской карты, которые вы вводите на своем компьютере.
- Когда вы получаете письма от сильно нуждающихся «королевских особ», которые за солидный процент просят вас перевести крупную сумму для спасения страны.

Как защититься:

- Не открывать сайты платежных систем по ссылке (например, в письмах), проверять, какой URL стоит в адресной строке.
- Совершайте покупки в интернете с помощью отдельной банковской карты и только на проверенных сайтах
- Никогда никому не сообщайте ваши пароли. Вводить пароли можно и нужно только на самих сайтах платежных процессоров.
- Не храните файлы с секретной информацией на доступных или недостаточно надежных носителях информации.
- Если вам предлагают удаленную работу и при этом просят оплатить взнос в качестве гарантии за пересылку данных и т. п., не попадайтесь на эту ловушку.
- Письма о проблемах с вашим счетом в какой-либо платежной системе, требующие перехода на сайт и каких-либо действий от вас, удаляйте.
- В 99 % случаев платежи, которые вы делаете онлайн, отменить нельзя. Поэтому не торопитесь, подумайте, прежде чем заплатить за товар или услугу.

По данным международной статистики, совокупные потери операторов связи и абонентов от **мобильного мошенничества** ежегодно составляют примерно 25 млрд долларов.

Вариантов их огромное множество, но основных видов не так много:

- «Вы выиграли приз...». При этом просит прислать подтверждающую СМС, внести «регистрационный взнос» через интернет-кошелек, купить карточку предоплаты и перезвонить, назвав код. Получив «взнос», мошенник исчезает, а обещанный приз тоже растворяется.
- «Мама, я попал в аварию», когда мошенник отправляет СМС или звонит с неприятной новостью, «жертва» в панике забывает проверить достоверность полученной информации и переводит средства на счета злоумышленников.
- «Блокировка карты». На мобильный телефон приходит СМС «Ваша банковская карта заблокирована. По вопросам разблокировки обращайтесь по телефону...». «Жертва» перезванивает по указанному номеру и «сотруднику банка», которым является мошенник, предлагает пройти к банкомату и совершить несколько операций под диктовку. Результат не заставит себя долго ждать - деньги с карты перейдут на счет мошенников.
- Рассылка вирусов, который помогает злоумышленникам подобраться к банковской карте, привязанной к мобильному телефону, и перевести все деньги на свой счет.

Способы защиты:

- Не отвечайте на СМС и не открывайте ММС от неизвестных абонентов, в том числе поздравительные сообщения и открытки.
- При получении сообщений от банков, мобильных операторов о проблемах со счетом перезвоните по известному вам номеру банка и уточните информацию.
- Не отправляете СМС на короткие номера, заранее не узнав стоимости подобного сообщения.
- Никогда не сообщайте никаких персональных данных, даже если вам звонят и представляются сотрудником банка, полиции, мобильных операторов и т. д. Попросите представиться, назвать ФИО, звание-должность, поинтересуйтесь, какой адрес у отделения, офиса, уточните наименование организации. Затем узнайте телефон этой организации и перезвоните.
- Вам могут позвонить и сообщить, что ваш родственник или знакомый попал в аварию, за решетку, в больницу - не верьте! Позвоните вашему родственнику.
- Ценную информацию никогда не храните только в телефоне, дублируйте ее в бумажном блокноте или в компьютере.

**Финансовая пирамида.** Чаще всего работает по следующему принципу: организаторы пирамиды собирают у вкладчиков деньги (продают ценные бумаги пирамиды), но не вкладывают эти деньги в экономику, а оставляют у себя. Они объявляют о росте курса своих ценных бумаг и, когда старые вкладчики хотят снять свои деньги с процентами, с ними расплачиваются деньгами новых вкладчиков.

Пирамиды обычно обещают сверхвысокую доходность: 200—300 % в год. Так как поначалу число вкладчиков всё время растёт, организаторы пирамиды могут какое-то время поддерживать её платёжеспособность.

Опасность пирамиды заключается в том, что рано или поздно она рухнет. Слишком много вкладчиков одновременно захотят продать свои ценные бумаги. Организаторы поймут, что расплатиться со всеми не получится, приостановят выплаты, а потом скроются с оставшимися деньгами.

### Как распознать пирамиду?

Во-первых, не поддавайтесь на агрессивную рекламу «легких и быстрых денег», гарантированная доходность выше ставки банковского депозита – повод задуматься о целесообразности таких вложений.

Во-вторых, обратите внимание на следующие признаки, которые могут характеризовать организацию как «финансовую пирамиду»:

- ✓ Вас призывают не раздумывать и вкладывать быстро
- ✓ Вам объясняют высокую доходность непрозрачными сверхприбыльными проектами, при этом не раскрывают информацию о потенциально возможных рисках. Проекты, как правило, находятся в другой стране, что затрудняет выяснение текущего положения дел.
- ✓ Организаторы скрывают информацию о себе, о наличии лицензий на ведение соответствующей деятельности и действуют через посредников. Часто компания зарегистрирована не в России, а в договоре отсутствует защита прав вкладчика

- ✓ Вам обещают высокое вознаграждения за приведенных друзей, знакомых или родственников. Предлагают построить систему привлечения клиентов и зарабатывать на ней. Агрессивно рекламируют свои услуги.

В-третьих, старайтесь принимать взвешенные финансовые решения, не поддавайтесь эмоциям жадности и страха.

Перед тем как отдать деньги:

- ✓ Проверьте наличие лицензии Центрального банка на ведение деятельности (банковская, страховая, инвестиционная).
- ✓ Внимательно изучите договор на предмет условий инвестирования и возврата средств.
- ✓ Найдите в сети Интернет информацию о данной организации, ее историю, отзывы клиентов, рейтинги в соответствующей отрасли.

Если деньги уже вложены в сомнительные проекты, постараитесь максимально оперативно изъять не только полученную прибыль, но и основные вложения. Не ждите, когда пирамида развалится, и не старайтесь компенсировать убытки, вкладывая новые средства.

Материал подготовлен в рамках Всероссийской недели сбережений 2019, которая проходит в рамках Проекта Министерства финансов Российской Федерации «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации». Узнайте больше на портале вашифинансы.рф.